A Goal VPN

Protection Profile

For

Protecting Sensitive Information

Release 2.0

10 July, 2000

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. AGENCY USE ONLY (Leave blank)	**2. REPORT DATE** 7/10/2000	**3. REPORT TYPE AND DATES COVERED** Report 7/10/2000

4. TITLE AND SUBTITLE
A Goal VPN Protection Profile for Protecting Sensitive Information

5. FUNDING NUMBERS

6. AUTHOR(S)
Information Assurance Solutions Program

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Booz Allen & Hamilton
8283 Greensboro Drive
McLean, VA 22102

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

National Security Agency

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; Distribution is unlimited

12b. DISTRIBUTION CODE
A

13. ABSTRACT *(Maximum 200 Words)*

This PP specifies the Department of Defense's (DoD) goal security requirements for protecting its own sensitive information. However, VPN technology may be used in many environments, both public and private. For instance, in the U.S. DoD an example of sensitive information is unclassified data that affect "Mission Support" operations, which are important to support deployed or contingency forces. Such data requires a "medium" level of robustness and security. However, without the inclusion of additional layers of security integrated to provide for "defense-in-depth," mechanisms specified by this protection profile are not sufficient for supporting a "high" level of robustness. This should also be true for non-DoD organization's sensitive information. Such material is any information deemed important to the organization, the loss of which might cause financial difficulties, schedule impacts, or affects the well being of employees. Security policies

14. SUBJECT TERMS
IATAC Collection, VPN, information, authentication, data protection, privacy

15. NUMBER OF PAGES
191

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT UNCLASSIFIED	**18. SECURITY CLASSIFICATION OF THIS PAGE** UNCLASSIFIED	**19. SECURITY CLASSIFICATION OF ABSTRACT** UNCLASSIFIED	**20. LIMITATION OF ABSTRACT** UNLIMITED

Protection Profile Summary

Background: This Protection Profile (PP) on Virtual Private Networks (VPNs) was generated under the Information Assurance Solutions program, sponsored by the National Security Agency (NSA). VPN technology was selected because it is an architectural solution that has gained prominence, and will become more pervasive in the future.

Terminology: VPNs use security mechanisms to effectively create a private network across a shared (usually public) communications backbone connecting distributed elements or members of a single organization. The interconnecting communications backbone may consist of leased lines, dial-up service, packet and cell switched connection-oriented networks, and/or routed connectionless networks. Also, VPNs are useful in restricting distribution among subsets of the organization at large. This type of nested VPN implementation is commonly referred to as a Community of Interest (COI) within an organization. Typically, VPNs may be utilized to securely communicate between:

- Site-to-site infrastructures across a public communications backbone. This may include Metropolitan Area Networks (MANs) and Building or Base Area Networks (BANs);
- Local Area Network (LAN)-to-LAN sub-nets operating across a network that services other entities outside the VPN community;
- Host-to-host workstations across a shared network or sub-net.

Scope: This PP does **not** reflect current VPN device technology. It represents the NSA's opinion of what functional security and assurance features near-term VPN implementations should incorporate; hence, it is referred to as a "Goal" VPN PP. Future releases of "Procurement" VPN PPs will detail compliance criteria for actual DoD VPN product procurements. We hope that VPN vendors will respond with products that meet the requirements of this PP and proceed to describe their products' security characteristics in the form of Security Targets (STs). [PPs and STs are specification documents defined in the International Common Criteria (CC). Details about this subject can be found on NIST, IATF and NSA web sites.]

Purpose: This PP specifies the Department of Defense's (DoD) goal security requirements for protecting its own sensitive information. However, VPN technology may be used in many environments, both public and private. For instance, in the U.S. DoD an example of sensitive information is unclassified data that affect "Mission Support" operations, which are important to support deployed or contingency forces. Such data requires a "medium" level of robustness and security. However, without the inclusion of additional layers of security integrated to provide for "defense-in-depth," mechanisms specified by this protection profile are not sufficient for supporting a "high" level of robustness. This should also be true for non-DoD organization's sensitive information. Such material is any information deemed important to the organization, the loss of which might cause financial difficulties, schedule impacts, or affects the well being of employees. Security policies for specific VPN implementations may dictate additional security requirements providing a higher level of protection than is specified by this PP. When a company's most sensitive information is to be sent over a publicly accessed network (e.g. the

Coke recipe while being distributed between manufacturing plants over the public network), the company should take other precautions to protect it.

Uses: This PP may be of use to several audiences, Information System Security Engineers (ISSEs), product vendors, security product evaluators, and system integrators. For ISSEs supporting the DoD community in designing secure information systems, this PP defines a goal set of security requirements for the protection of unclassified, sensitive information from which a specific implementation of a VPN can be designed and built. For product vendors and evaluators, this PP defines the system level requirements that should be addressed and documented in vendor STs. System integrators may find this PP useful in identifying areas that need to be addressed to provide secure system solutions. By matching the PP with available STs, security gaps may be identified and products, policies and procedures may be established to bridge these gaps. Readers of this PP must be cautioned, however, to not believe that this or any other PP provides a cook-book methodology for selecting components which, when integrated together, automatically result in validated system security solutions. As was recently pointed out in NSA, Deputy Director for Information System Security, "Information Assurance Advisory No. IAA-003-1999,"[1] "There are no perfect security solutions, and no particular product in and of itself will provide risk-free security."

Method of Analysis:

The authors considered several applicable policy, guidance, and architectural documents to specify goal security requirements for the application of VPN technology. These include the Information Assurance Technical Framework Forum's "Information Assurance Technical Framework"[2] document, the "X.509 Certificate Policy for the United States Department of Defense"[3] and the Department of Defense Chief Information Officer Guidance and Policy Memorandum No. 6-8510 "Department of Defense Global Information Grid Information Assurance"[4].

The authors first considered the environment in which VPN devices typically are used and subsequently defined two specific environments. The first is one we call the Operational User (OU) site; the second, the Remote User (RU) site. An OU site is defined as a controlled facility physically protected with access limited to Authorized Users and authorized System and Security Administrators. Site administration is provided by clearly identified, well trained (typically resident), authorized System and Security Administrators. The RU site is external to a controlled facility, yet tied to a "home" site. It is a computer operated by an Authorized User or System or Security Administrator who is "on the road". Physical protection is typically limited and is

[1] "Information Assurance Advisory No. IAA-003-1999," subject: "Information Assurance (IA) – More Than Evaluated Products," dated 3 November 1999, and signed by Michael J. Jacobs, Deputy Director for Information System Security

[2] "Information Assurance Technical Framework," Release 2.0.1, September 1999, Issued by the National security Agency, Solution Development and Deployment, Technical Directors

[3] "X.509 Certificate Policy for the United States Department of Defense", dated 13 Dec 1999

[4] Department of Defense Chief Information Officer Guidance and Policy Memorandum No. 6-8510 "Department of Defense Global Information Grid Information Assurance", dated 16 Jun 2000

usually compared to the protection provided to “high-valued” equipment or assets such as a personal computer.

The authors defined threats, assumptions and organizational policies that should be addressed by VPN devices and related components operating in these environments. Then, they derived the implementation independent security objectives of the VPN system, as well as the functional security and assurance requirements. Finally, they developed the rationale for the proposed security objectives and requirements.

Threats, policies, and assumptions: The PP identified 27 threats, 21 policies and deduced 16 assumptions related to the security aspects of the described functionality and applicable environment. The threats to a site’s assets are those that our security analysis found to be applicable to both the OU and RU implementations and relevant to the entire environment at both the OU and RU sites. Relevant threats are documented in section 3.1, policies in section 3.2 and related assumptions in section 3.3.

Security Objectives: The threat, policies and assumptions analysis led to 25 security objectives for the VPN device and 18 for the environment (no effort was made to ensure completeness for the environmental objectives, because that is not the purpose of this PP). These security objectives are documented in section 4. Collectively the security objectives:

- provide confidentiality and integrity protection for unclassified data and user identity as the data moves from an unclassified, sensitive environment through a shared communications backbone to another unclassified, sensitive environment;
- remove confidentiality protections from peer devices, verify integrity of data between peer VPN devices, and remove integrity mechanisms from the protected (unclassified), sensitive data as it moves from the shared network environment to the receiving sensitive environment;
- provide mechanisms to restrict the use of the VPN device to Authorized Users, administrators and devices within an OU site (as identified by IP addresses and passwords);
- provide authentication mechanisms which restrict the receiving VPN device to process only information generated by selected VPN peers;
- provide a limited auditing and alarming capability to record and report VPN related security events (e.g. security connection establishment/termination, failures, and errors);
- provide local and remote interfaces for VPN administration;
- support standards-based network operations.

Security Requirements: Once objectives were identified, the authors chose the security functional requirements, as specified by the CC, that satisfy these objectives. They are as follows:

Operational User Site

- **Audit:** This CC requirement class involves recognizing, storing, and analyzing information related to security relevant activities. The authors selected alarming, audit generation, audit review and selective audit. We did not require storage or analysis because we assumed that this would be external to the VPN mechanism and incorporated in a function we defined as Misuse Detection (MD) located within the system security environment.

- **Cryptographic support:** This CC requirement class involves cryptographic functionality (such as encryption, hashing, authentication, data integrity, and key management) that may be utilized in security mechanisms such as identification and authentication (I&A), non-repudiation, trusted path and channel, and data separation. Detailed cryptographic guidance is provided in section 5.1, under the FCS CC requirement class. Most mechanisms recommended followed logically once the authors chose 3DES as an encryption algorithm. This point is discussed in some detail in Section 6.4, "Minimum Strength of Function Argument". Only currently available commercial mechanisms were considered and the authors chose those that are "standard", commonly recognized, or in wide use.

- **User data protection:** This CC requirements class specifies security requirements for the VPN's functions and policies as they relate to protecting user data. Presently, VPNs receive bits, encrypt or decrypt them, and ship them to either another VPN or the Authorized User. The authors believe more care is necessary to ensure that a given VPN is communicating with an authorized VPN and, hence, Authorized Users. Therefore, the requirements we selected ensure that VPNs provide confidentiality and integrity protection, source authentication, replay prevention, and user access control. Some of these selections fall into the category of security goals, which are not commonly implemented, in current VPN products. However, the authors believe that the selected requirements are implimentable with available technology and should be incorporated in near-term VPN products.

- **Identification and Authentication (I&A):** This CC requirement class addresses the need for security functions that establish and verify claimed user identification. Like the previously discussed user data protection requirements, current VPN mechanisms rarely incorporate the level of detail specified in these goal requirements. Once again the authors have identified I&A requirements that they believe are achievable and necessary in near-term system implementations. Requirements specified in this CC requirement class include authentication failure handling, user attribute definition, key generation and enforcement, user I&A, and continuous data authentication.

- **Security management:** This CC requirements class relates to security issues involved in managing the VPN device itself. It includes security functions such as banners for printouts, access control lists, and mechanisms that specify user roles.

The authors placed in the hands of only System and Security Administrators the ability to manage security functions, values of security attributes, and setting security default options. Thus, the Administrators will have split roles in creating and managing access control lists, setting audible events, managing the audit records, managing backup, and the like. This responsibility led the authors to require X.509 certificates to identify and authenticate Administrators, while allowing the users to be I&A'd via passwords and IP addresses only. The authors recommend that the VPN of the future recognize and enforce the different roles of administrators and users.

- **Privacy:** This CC requirements class provides users protection against the discovery and the misuse of identity by other users. The authors selected only anonymity and unobservability, and both at a basic level. Thus, the VPN device must ensure that parties on public networks are unable to determine the real user name bound to datagrams emanating from the device. Also, it must provide the System and Security Administrators with the capability to observe the use of VPN resources and processes.

- **Protection of the device security functions:** This CC requirements class contains functional requirements that relate to the integrity and management of the VPN device's security mechanisms versus the User Data Protection Class discussed earlier. User Data Protection focuses on user's data, while protection of device security functions focus on the VPN device's data protection. The authors specified requirements such as preserving a secure state, data integrity, automated recovery, and domain separation.

- **Resource utilization:** This CC requirements class supports the availability of required resources (e.g. processing and storage). The authors require that VPNs default to a secure state upon detecting failures, and enforce that individual users cannot dominate the VPN over any period of time.

- **VPN device access:** This CC requirements class specifies requirements for controlling a user's session. The authors limited the number of concurrent sessions by a user and required that the VPN device terminate an inactive session (parameters established by administrator command). The use of the VPN is permitted based on valid user IP address, password or valid System or Security Administrator authentication identities.

- **Trusted channels:** This CC requirements class requires the creation of a trusted channel between the VPN device and other trusted products in the security environment. This class is included to ensure secure communication between the VPN device and other security components such as an audit analysis tool (Misuse Detection system) or key management infrastructure. The authors require a secure communication channel between products that are logically distinct, assured identification of its end points, and protection of the channel from unauthorized data modification or disclosure.

Remote User Site

The RU site VPN has the same requirements as those for the Operational User site **except**:

- The remote user may assume the role of an administrator. Therefore, the RU functional requirements occasionally allow for this role difference in several of the classes.

- Remote users have the added protection of a hardware token for activation of their local VPN mechanisms while at an OU site users identify themselves to a shared VPN boundary mechanism by means of unique passwords and IP address associated with an Access Control List (ACL). This difference is reflected in the cryptographic and I&A CC requirements classes.

- Quota limitations were not included in the resource utilization class, because there is only one user at a RU site.

Assurance level: The authors selected an assurance level of EAL 3 (Evaluated Assurance Level 3) (augmented with one additional requirement to develop an informal security policy model) after considering existing policy recommendations regarding robustness of mechanisms to protect sensitive information. They decided on this assurance level after considering the IATF produced robustness strategy (referenced earlier) and after careful consideration of the data these devices must protect. A detailed discussion of this issue is contained in section 6.3. EAL 3 plus the recommended additional requirement are summarized in Table 3.

Summary of Interesting and (perhaps) Surprising Recommendations

- *Requiring that VPNs of the future operate at both the application (on the high side) and network layers (on the low side) of the ISO stack* - Presently, users may not even be aware that a VPN might be protecting them. They operate transparently at the network layer. However, moving to the application layer allows for additional useful, security functionality that includes robust checking of users prior to their use of system resources (release authority concept), enforcing roles among users and administrators, allowing for COI (Communities of Interest), and enforcing compartmentation.

- *Requiring split roles for System and Security Administrators* - The authors levied this rather than forcing using organizations to assume away the possibility of a corrupt administrator. Administrators of modern computer systems have enormous power to harm (or help) an organization.

- *Recommending "Misuse Detection"* - Organizations should consider environmental functionality that we term "Misuse Detection" that is discussed in Appendix B of the PP.

- *Recognizing use of RU site software-based VPNs* - In the case of a remote user communicating with his home site, he most probably will do so with a software based VPN client, because that is what is typically available in the marketplace. In these cases the operating system should be trusted as appropriate for FIPS 140-2 level 2 compliance.

- *Use of Special Purpose Device* - The OU VPN device is a Special Purpose Device (SPD) and consequently will not execute general-purpose programs. An SPD is a combination of computer hardware and software that limits either, the functionality or the use of the device (see Terminology section of the PP).

- *Strong, remote authentication* – Hardware tokens are required for both users and administrators when at a remote site.

- *Local authentication* - Weaker authentication is permitted for local (OU site) users but not administrators.

Table Of Contents

List of Figures

List of Tables

Table # Title Page #

Conventions and Terminology

Conventions

The notation, formatting, and conventions used in this protection profile (PP) are based on or consistent with version 2 of the Common Criteria (CC). Font style and clarifying information conventions were developed to aid the reader. Additionally, British English has been used in sections of the protection profile drawn directly from the Common Criteria standard language.

The CC permits four functional component operations—assignment, iteration, refinement, and selection—to be performed on functional requirements. These operations are defined in Common Criteria, Part 2, paragraph 2.1.4 as:

- assignment: allows the specification of an identified parameter;
- refinement: allows the addition of details;
- selection: allows the specification of one or more elements from a list; and
- iteration: allows a component to be used more than once with varying operations.

These operations are expressed by using **bolded**, *italicized*, and underlined text as specified in Table 1.

Additionally, brackets ("[ ]") are used to set off all assignments or selections that are left to be specified by the developer in subsequent security target documentation. In addition, when an assignment or selection has been left to the discretion of the developer, the text "assignment:" or "selection:" is indicated within the brackets.

Table 1 Functional Requirements Operation Conventions

Convention	Purpose	Operation
Bold	**Bolded text** is used to indicate that new text has been added as part of either an assignment or refinement operation to the CC standard language. CC standard language: FDP.ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following rules: [assignment: *rules, based on security attributes, that explicitly authorize access of subjects to objects*.] CC assignment operation example: FDP.ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following rules: **valid key exchange**	Assignment or Refinement
Italics	*Italics* are used to indicate that the included text has been selected from a list of options provided in the CC standard language. CC standard language: FIA.UAU.3.1 The TSF shall [selection: *detect, prevent*] use of authentication data that has been forged by any user of the TSF. CC selection operation example: FIA.UAU.3.1 The TSF shall *prevent* use of authentication data that has been forged by any user of the TSF.	Selection
Underline	The purpose of underlined text is to inform the reader that the CC component has been iterated to allow for more than one usage with varying assignment or selection operations.	Iteration

Application Notes: To provide support information that is considered relevant or useful for the construction, evaluation, or use of the TOE, (e.g., to clarify the intent of a requirement, to identify implementation choices, or to define "pass-fail" criteria for a requirement) “Application Notes” are used. Application notes related to a set of functional or assurance components, are included following the relevant requirement component.

Example:

> **Application Note:** There is no intent to require the TOE to store audit records. What is required is for the TOE to cryptographically sign the audit record…

Assumptions: TOE security environment assumptions are given names beginning with "A." and are presented in alphabetical order.

Examples:

A.ADMIN At an OU site there are resident System and Security Administrators. At an RU site, administration is provided by assigned home site System and Security Administrators, but sometimes is implemented by the Remote User at the RU site. Administration responsibilities will be split between a System Administrator and a Security Administrator who together will be able to administrate the entire system. This is done to prevent any one person having too much control and to provide for "checks and balances."

A.ADMIN_SECURITY_RESTRICTED - Restrictions exist outside the TOE, but within the TSE, to allow only System and Security Administrators to administer security devices.

Threats: TOE security environment threats are given names beginning with "T." and are presented in alphabetical order.

Examples:

T.ATTACK_DATA - The TOE will encounter data that may contain malicious code. An Authorized User or Unauthorized Agent may use malicious code to attempt to disrupt site security operations or the TOE itself.

T.BAD_ACCESS_INAPPROPRIATE - Authorized Users may intentionally or unintentionally access or modify information, or utilize resources for which they are not approved.

Policies: TOE security environment policies are given names beginning with "P." and are presented in alphabetical order.

Examples:

P.ACCOUNT Users, and System and Security Administrators must be held accountable for security relevant actions.

P.ADMIN_SECURITY_RESTRICTED - Only Authorized System and Security Administrators and approved maintainers may administer or repair devices in the TSE.

Objectives: Security objectives for the TOE and the TOE environment are given names beginning with "O." and "OE." respectively and are presented in alphabetical order.

Examples:

O.ADMIN The TOE must provide functions to enable System and Security Administrators to effectively manage the TOE and its security functions, ensuring that only they can access administrative functions.

OE.INFO_SECURITY_OFFICER – An Information Security Officer will be identified who will be responsible for creating, maintaining, interpreting and overseeing consistent implementation of site security policy and procedures.

Terminology

Common Criteria, Part 1, Section 2.3 provides a glossary of relevant terms, some of which are listed here to aid the reader. Several of the Common Criteria provided terms are further clarified and additional terms have been included and defined in the following list:

Administration - Administrative responsibilities will be split between a System Administrator and a Security Administrator who together will be able to administer the entire system. This is done to prevent any one person having too much control and to provide for two person integrity (checks and balances).

Authorized User - Any person (or process acting on behalf of a person) who is outside the boundary of the Target of Evaluation (TOE), who is authorized to interact with the TOE. Authorized Users (AUs) are trusted. However occasionally they may prove themselves to be untrustworthy, in which case they are referred to as an Unauthorized Agent (UA).

Community of Interest - A Community of Interest (COI) is a subset of AUs that either communicate within, or between, Operational User (OU) and Remote User (RU) sites. Communications among and between COI AUs will be protected from both access and modification by non-COI AUs or UAs.

COI Authorized User - Any person (or process acting on behalf of a person) who is outside the boundary of the TOE, who is authorized to interact with the TOE, and who has additional authorization to access or modify information and utilize resources that has been designated to be within the COI. COI AUs are trusted. However, occasionally they may prove themselves to be untrustworthy, in which case they are referred to as UAs.

Component The smallest selectable definition of a CC functional requirement. When a CC component is included in a PP or ST, all associated CC component elements are also included.

Dependency A relationship between requirements such that the requirement that is depended upon must normally be satisfied for the other requirements to be able to meet their objectives.

Element Most detailed refinement of a CC functional requirement. Similar elements when grouped together form a CC component requirement. When a CC component functional requirement is included in a PP all associated elements must be included.

Evaluation Assurance Level (EAL) - A collection of assurance components from CC, Part 3, which when selected together represents a point on the CC predefined assurance scale.

External communication channel - Communication links between TOE Security Environments (TSEs) and external Information Technology (IT) systems or entities.

Information Defined as user data, regardless of its format.

Information Security Officer (ISO) - A person responsible for creating, maintaining, interpreting and overseeing consistent implementation of site security policy and procedures.

Internal communication channel - Communication links internal to the components of the TSE (e.g. Operational User (OU) site, Remote User (RU) site, or sensitive information site with COI).

IPSec (Internet Protocol Security – IPSec is a framework for a number of security specifications pertaining to VPNs. IPSec's three core components were ratified by the Internet Engineering Task Force (IETF) in 1998. They are:

1. The authentication header (AH) which verifies the authenticity of the packet's contents;
2. The encapsulating security payload (ESP) that encrypts a packet before transmitting it. ESP may also encapsulate the original IP packet; and
3. The Internet Key Exchange (IKE) which governs the exchange of security keys between senders and receivers. The IKE endorsement subsumes what used to be referred to as ISAKMP/Oakley standard.

Misuse Detection (MD) - A set of mechanisms (processes and components) that perform several specialized functions such as virus checking, intrusion detection, examining various aspects of the material being transmitted for unauthorized content, analyzing characteristics of user profiles for "normalcy", analyzing audit records, and alerting operational personnel when misuse is detected or suspected.

Operational User (OU) – An employee who functions within an organization's spaces (usually with some protection…see Operational User Site, 2.3.1). Typically the OU's job is directly related to the mission and functions of that site. OU's are subject to the supervision (either directly or indirectly) of a senior official at the site.

Periods Processing – A technique to process different levels of data by separating the operation of the computer system into time slots, changing out software and hard drives and employing other such techniques to ensure secure operations.

Protection Profile (PP) - An implementation-independent set of security functional and assurance requirements for a category of devices (TOEs) that meet specific consumer needs. Recently, NSA defined two types of PPs: 1. A "Goal PP" specifies requirements for security devices that are independent of what currently exist on the market place; and 2. A "Procurement PP" specifies requirements for devices that may be purchased off-the-shelf currently.

Private Network – A dedicated network of leased lines for the typical purpose of conducting site-to-site or business-to-business communications privately, reliably, and efficiently.

Public Network – The system of publicly accessable, shared networks, such as the Internet, over which may flow a variety of data types such as voice, facsimile, video, and computer generated data and graphics.

Remote User (RU) - An Authorized User (AU) of the RU site.

Resources Any system asset required for the correct operation of the TSE.

Security Target (ST) - A set of security requirements and specifications to be used as the basis for evaluation of an identified TOE.

Security Administrator - Human user (outside the boundary of the TOE) to whom authorization has been granted to perform security administrative operations which affect the enforcement of the site's TOE security policy (TSP). The Security Administrator defines auditable events, may modify audit data, assigns privileges to AUs, defines access control lists (ACLs), defines peer TOE ACLs, and performs other security duties as defined by the site's security policy and ISO. Security Administrators are trusted. However, occasionally they may prove themselves to be untrustworthy, in which case they are referred to as an UA.

Sensitive information – Information that requires protection, because the information's content is either sensitive or distribution is restricted. Loss or modification of the sensitive information may cause damage to the security, safety, financial posture, and/or infrastructure of the organization. Organizations, both inside and outside of government seek to protect information of this type. For example, in a DoD environment sensitive information might be information related to the provisioning of military supplies such as bullets or fuel to deployed forces. "Sensitive information" as used herein, is unclassified, more important than routine administrative information, and less important than mission critical information.

Special Purpose Device (SPD) - A combination of computer hardware and software that limits either, the functionality of the device, or who can use the device. Typically, the manufacturer of the device modifies standard equipment and software to ensure that the SPD carries out its designated purpose. Some techniques used to ensure that an SPD is safe and limits functionality or use are:

- Removal of sections of the COTS operating system (OS) or replacing the COTS OS with a special, customized version;
- use of ROM versus RAM to store programs and data;
- use of state features of a multi-state machine to control where executables must reside, or;
- some combination of these techniques.

Each manufacturer that claims a device is an SPD must document how they control the specialization of the device.

System Administrator - Human user to whom authorization has been granted to perform generic administrative operations, some of which may affect the enforcement of the TSP. The System Administrator registers users, performs system back ups, establishes host addresses and performs other duties as defined by the site's procedures, site security policy and ISO. System Administrators are trusted, however occasionally they may prove themselves to be untrustworthy and knowingly violate the site security policy, in which case they are referred to as an UA.

Target of Evaluation (TOE) - An IT product or system, and its associated administrator and user guidance documentation, which is the subject of the PP definition of functional and assurance requirements (and in a ST, the subject of an evaluation.)

TOE Security Functions (TSF) - A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TOE Security Policy (TSP.)

TOE Security Policy (TSP) - A set of rules that regulate how assets are managed, protected, and distributed within a TSE. .

TSF Scope of Control (TSC) - The set of interactions that can occur with or within a TOE and are subject to the rules of the TOE site security policy.

Unauthorized Agent (UA) - Any person (or process acting on behalf of a person) that is not authorized, under the TOE site security policy, to access the TOE resources or information processed by the TOE. This person includes anyone from a "hacker" to a determined foreign adversary, and Security Administrators, System Administrators or Authorized Users who are untrustworthy, do not possess COI privileges or lack the need to know.

Virtual Private Network – A network that is secured by using cryptographic techniques to provide communication between users across networks with unknown security. It is called "virtual private" because the organization utilizing this technology achieves private network security on a public backbone.

Document Organization

Section 1 Introduction, provides document management and overview information necessary to identify the PP and clarify its scope and appropriate application. It also references other related PP documents. .

Section 2 Target of Evaluation (TOE) Description, defines the TOE and establishes the context of the TOE both generically and by referencing a specific customer's (Navy VPN) set of generalized requirements.

Section 3 TOE Security Environment (TSE) further refines the explanation of the TOE by describing typical applications of the TOE in the context of its surrounding environment, the TSE. The TSE describes the application of VPN technology, which has been considered in developing the PP system level functional and assurance security requirements. The TSE description includes a discussion of the expected environments for using VPN technology and clarifies it in terms of applied site security policy, applicable threats, and security usage assumptions.

Section 4 TOE Security Objectives, defines the sets of security objectives for both the TOE and the TOE environment which are based on a consideration of the defined threats, policy and assumptions.

Section 5 IT Security Requirements, contains an itemization of the TOE functional and assurance requirements which have been derived from the Common Criteria, Part 2 and 3, respectively.

Section 6 Rationale, contains an explicit explanation of how the identified TOE security objectives address the identified relevant threats and policies. Arguments are provided for the coverage of each policy and threat. The section then explains how the set of requirements are complete relative to the objectives, and that each security objective is addressed by one or more component requirements. Arguments are provided for the coverage of each objective. Next Section 6 provides a set of arguments that address dependency analysis, strength of function issues, and the internal consistency and mutual supportiveness of the protection profile requirements.

An acronym list is provided to spell out frequently used Common Criteria acronyms.

A reference section is provided to identify background material.

1. Introduction

This Protection Profile (PP) was generated under the Information Assurance Solutions program, sponsored by the National Security Agency (NSA). The Information Systems Security Organization of NSA decided to prepare a PP focused on Virtual Private Networking (VPN), which documented the goal functional and assurance requirements appropriate for both DoD and public sector usage.   VPN technology was targeted because it is an architectural solution that is gaining prominence, and will become pervasive in the future. The Information Assurance Technical Framework (IATF) document, originally drafted by NSA with input from both industry and civil agencies, devotes an entire chapter to VPN usage (Release 1.1," section 5.2, "System High Interconnections and Virtual Private Networks"). The properties the PP team felt necessary to mandate in compliant VPN products and systems include confidentiality, data origin authentication, connectionless integrity, protection from data replay attacks, and limited traffic flow security (e.g. equivalent to the security provisions incorporated in the draft IPSec standard). In addition to the traditional security functions associated with VPNs, the PP team has included requirements in this PP which mandate identification and authentication (I&A) of authorized user client applications and administrators to the VPN function. These additional requirements resulted from the team's opinion that VPN based solutions typically also include requirements for plain text bypass, remote administration and support for limited access (Community Of Interest, COI) all of which require I&A support.

This PP may be of use to several audiences, Information System Security Engineers (ISSEs), product vendors, security product evaluators, and system integrators.

- For ISSEs supporting the Department of Defense (DoD) community in designing secure information systems, this PP defines a minimal set of security requirements for the protection of unclassified sensitive information upon which a specific implementation of a VPN can be built.

- For product vendors and evaluators, this PP defines the system level requirements that must be addressed by provided products as documented in vendor Security Targets (STs) and as evaluated.

- For system integrators this PP is useful in identifying areas that need to be addressed to provide secure system solutions. By matching the PP with available STs, security gaps may be identified and products or procedures may be configured to bridge these gaps.

Section 2 of this PP uses a military example to describe a typical use of VPNs. Note however, that VPN technology may be used in many environments, both public and private. Additionally, VPN technology may be used on its own or in conjunction with other security mechanisms to provide a layered security architecture addressing many levels of required security assurance or robustness.

Identification: ______________

Title: Virtual Private Network Protection Profile for Unclassified Sensitive Environments

Authors: Mike Sheridan, Eliot Sohmer, Ron Varnum

Contributors: Cheryl Agro, Kris Britton, Tho Nguyen, David Opitz, Margaret Salter, and Marvella Towns. **Vetting Status:** <In process>

CC Version: This Protection Profile (PP) was developed using Version 2.0 of the Common Criteria (CC).

General Status: Active

Registration: <TBD>

Keywords: VPN, security, application, COTS, encryption, protection profile, network security, crypto bypass.

1.1 Protection Profile Overview

This Protection Profile specifies the Department of Defense's (DoD) near-term, "goal" (see terminology section, "Protection Profile") security and architectural requirements for protecting its own sensitive information utilizing VPN technology. In the U.S. DoD an example of sensitive information is unclassified data or mission information, which is important to support deployed or contingency forces. For non-DoD environments, sensitive information is any information deemed important to the organization, the loss of which might cause financial difficulties, schedules impacts, or affect the well being of employees. Organizations both in and out of government have this type of information to protect.

For the purposes of specifying the near-term goal security requirements for the application of VPN technology, the authors of this PP have generally considered the single layer of VPN protection offered independent of other layers of a total security architecture. However, in specifying the functional and assurance security requirements related to the VPN Target of Evaluation (TOE) (which are typically implemented within layer 3 of the OSI model), this PP has also included the requirement for (I&A) of authorized user client applications and administrator access to the VPN function. These additional requirements, which typically reside within layer 7 of the OSI model, resulted from the team's opinion that VPN based solutions typically also include requirements for plain text bypass, remote administration and support for limited access (Community Of Interest, COI) all of which drive the need for I&A support.

The target robustness level considered in this PP is "medium" as specified in the US DoD "Guidance and Policy for Department of Defense Information Assurance[5]". Use of such mechanisms is appropriate for applications handling important or sensitive data (unclassified only) or protection of system-high information in a low to medium risk environment such as the SIPRNET. As intreputed from the DoD guidance document, VPN technology offering a "medium" level of robustness and security strength is appropriate for "Mission Support"

[5] Department of Defense (DoD) Chief Information Officer, Guidance and Policy Memorandum No. 6-8510 "Department of Defense Global Information Grid Information Assurance", dated 16 June, 2000.

operations (i.e. use in DoD systems handling information that is merely sensitive; may be important to the support of deployed or contingency forces; must be absolutely accurate, but can sustain minimal delay without seriously affecting operational readiness). Without the inclusion of additional layers of security, integrated to provide for “defense-in-depth, mechanisms specified by this protection profile will not be considered sufficient for supporting “Mission Critical” operations or systems requiring a “high” level of robustness.

In either a public or private, non-DoD environment, mechanisms specified by this PP are appropriate for protection of both administrative information, and information related to private, sensitive, day-to-day operations. When a company’s most sensitive distribution information is to be sent over a publicly accessed network (e.g. the Coke recipe while being distributed between manufacturing plants over the public network), the company should apply additional layered security mechanisms.

Site security policies for specific VPN implementations may dictate additional security requirements providing a higher level of protection than is specified herein. This PP defines the threats, assumptions and organizational policies that are to be addressed by a VPN system. It defines the implementation independent security objectives of the VPN system and its environment, as well as the functional security and assurance requirements. Finally, the PP provides the rationale for the proposed security objectives and specified security requirements.

Readers of this PP must be cautioned however, to not believe that this or any other PP provides a cook-book methodology for selecting components which when integrated together automatically results in validated system security solutions. As was recently pointed out in NSA, Deputy Director for Information System Security, “Information Assurance Advisory No. IAA-003-1999[6],” “there are no perfect security solutions, and no particular product in and of itself will provide risk-free security.”

The entire text of IA Advisory No. IAA-003-1999[6] reads as follows:

Subject: Information Assurance (IA) – More Than Evaluated Products

Significant efforts have been expended over the past several years to develop and implement processes for evaluating and validating the performance characteristics of both commercial and U.S. Government Information Assurance (IA) products. There continues to be a misconception that these processes will “magically” result in the generation of a list of products that, when acquired and installed, will provide guaranteed security for the systems in which they are used. Nothing could be further from the truth. There are no perfect security solutions, and no particular product in and of itself will provide risk-free security. Buyers and users of IA products must understand that IA is more than just buying the right product. Rather, it must be a managed process which includes the acquisition of evaluated and validated products; risk management considerations which factor in the sophistication of the threat; an analysis of the

[6] “Information Assurance Advisory No. IAA-003-1999,” subject: “Information Assurance (IA) – More Than Evaluated Products,” dated 3 November 1999, and signed by Michael J. Jacobs, Deputy Director for Information System Securi

system(s) in which the products will be used; proper installation, integration and testing of acquired products; and post installation system certification and accreditation procedures. Additionally, trained and disciplined system administrators and network managers are key to success. System configuration changes must be carefully managed and documented to assure continued security.

Even with the successful accomplishment of the above steps, there will always be residual risks, including the insider threat. System users, operators and administrators must be constantly vigilant to changing threat and new vulnerabilities, which may negate the intended security services of IA products. In that context, IA should never be viewed as a destination, but rather a continuing journey of assessment and reassessment to ensure the security and integrity of systems and information they process.

1.2 Related Protection Profiles

Application-Level Firewall Protection Profile – The Application-Level Firewall Protection Profile (PP) may be related to this PP because it represents a candidate set of additional network boundary protection requirements. These additional requirements may be appropriate to supplement the requirements identified in this PP, when creating a total, sensitive, system-high, network solution for specific user applications.

Remote Access Protection Profile - The Remote Access Protection Profile (PP) documents requirements for protecting sensitive information communicated between a remote user and his/her home site via the public switched telephone network (PSTN). This VPN PP addresses the PSTN connectivity case as well as packet switched connectivity via the Internet. The Remote Access PP may offer alternative options that should be considered by system security designers when composing total system solutions.

2. TOE (Target of Evaluation)

Virtual Private Networks (VPNs) use security mechanisms to effectively create a private network across a shared (usually public) backbone. Prior to the wide dissemination of Internet technology, networking between separate parts of an organization required a privately owned system of communications lines or the leasing of fixed telecommunications services between the various entities. VPN technology offers a lower cost alternative that is much more flexible in terms of adding and removing nodes from the "virtual network." Also, VPN technology offers a decreased risk of exposure of the organization's sensitive information, because the information, formerly exposed to the shared backbone, is now placed in a virtual "tunnel" by means of providing an encrypted path between separated organizational enclaves.

The purpose of a VPN is to protect important information when using a shared communications infrastructure. The communications infrastructure may consist of leased lines; dial-up service, packet and cell switched connection-oriented networks, and/or routed connectionless networks. Also, some VPNs are useful in implementing Community of Interest (COI) enclaves within an organization.

2.1 Connectivity Options for Applications of VPN Technology

Figure 1 depicts three different applications for implementing VPN technology within a network environment. These connectivity options have been previously described in the "Information Assurance Technical Framework[7]" document (formerly known as the Network Security Framework document).

- Site-to-site VPNs connect major infrastructures across a public communications infrastructure. This may include Metropolitan Area Networks (MANs) and Building or Base Area Networks (BANs).

- Local Area Network (LAN)-to-LAN VPNs connect sub-nets together across a network that services other entities outside the VPN community.

- Host-to-host VPNs connect workstations across a shared network or sub-net.

All three of these VPN applications result in the connection of separated discrete enclaves, subgroups or individuals in such a manner as to provide unimpeded communications between them. The VPN application between the separated entities of the organization must, provide for the authenticated origin of the transmitted information, ensure the integrity of the information as it is transmitted, deny access and provide privacy to the information as it is tunneled through the public network and ensure that adversaries don't impersonate legitimate transmissions by replaying old ones.

[7] "Information Assurance Technical Framework," Release 2.0.1, September 1999, Issued by the National Security Agency, Solution Development and Deployment, Technical Directors

A remote access workstation networking into any of these three is a special case of either the host-to-host configuration or a hybrid of the host-to-host and LAN-to-LAN (i.e., host-to-LAN). In all these connectivity options, the security service requirements are very similar. However, the threats and countermeasure mechanism requirements may differ given the environmental constraints and attributes associated with a VPN implementation.

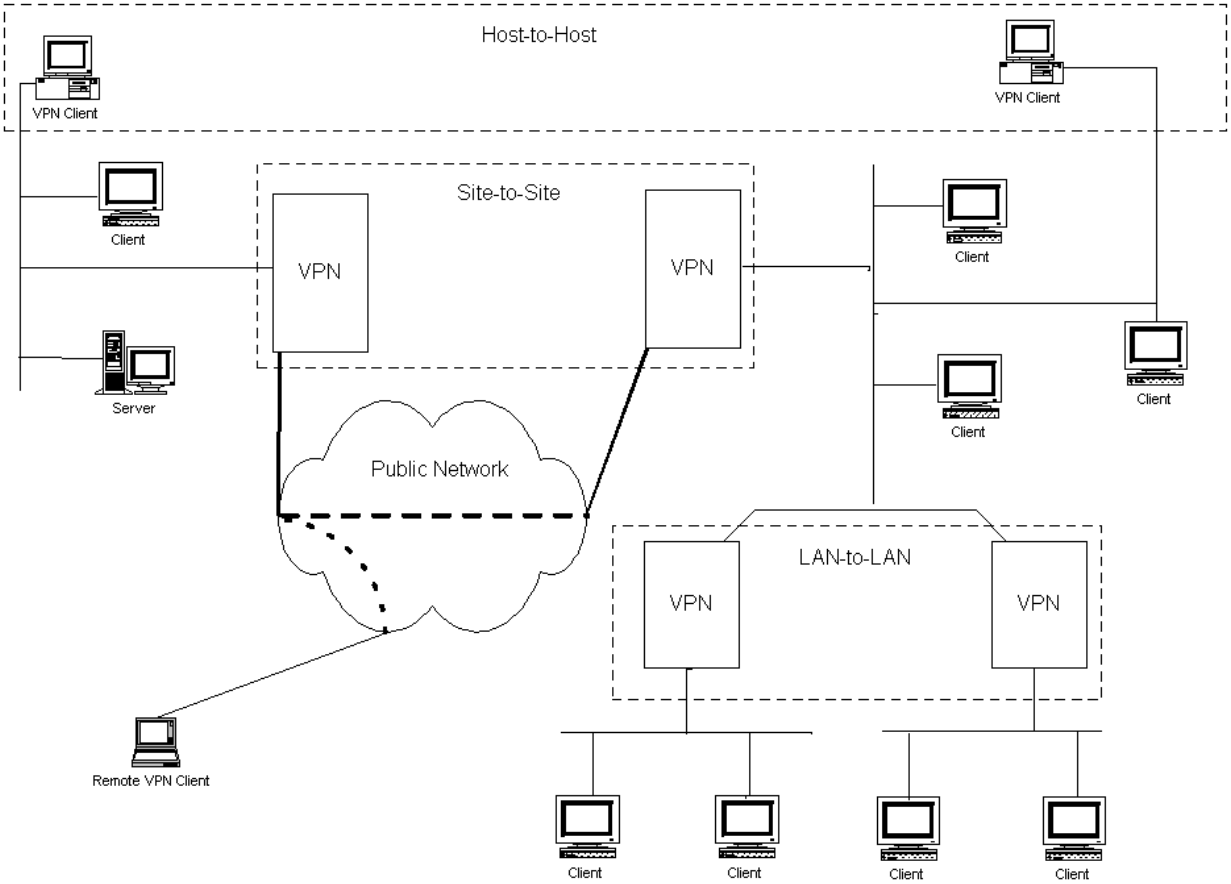

Figure 1 Application of VPN Technology

2.2 The TOE (Target of Evaluation)

For the purpose of this protection profile, the TOE is defined as a VPN device (or software application) that connects entities within unclassified sensitive system-high environments over a publicly accessible, shared network (Public Network) environment. Its purpose is to:

- provide confidentiality and connectionless integrity protection for unclassified sensitive data and user identity as they move from an unclassified sensitive environment through the shared network environment to another unclassified sensitive environment;

- upon receipt from peer TOE devices remove confidentiality protection, verify integrity of received data and remove the integrity related information from the protected (unclassified) sensitive data as it moves from the shared network environment to the receiving sensitive environment;

- provide mechanisms to limit the use of the TOE to authorized local users (identified by IP addresses and associated passwords) and remote users or administrators (both identified by associated hardware tokens);
- protect against adversaries' attempts to disrupt or corrupt data transmission by replicating previous transmissions;
- provide limited traffic flow confidentiality protection;
- provide authentication mechanisms which restrict the receiving TOE to process only information transmitted by selected TOE peers;
- provide a limited auditing and alarming capability to generate audit records (for external TOE analysis) and respond to identified TOE related security events (e.g. security connection establishment/termination, failures, and errors);
- provide for directly connected (local hard-wire connection) and remote (over the network) interfaces for TOE administration;
- support standards-based network operations.

The TOE is contained within its associated security environment which, is referred to as the TOE Security Environment (TSE).

2.3 An Example: The Navy VPN Generic Site Requirements

An example of a typical VPN application is the Navy SPAWAR initiative, which has identified the three configurations depicted in Figure 2. The configurations in which VPN technology is incorporated are identified as an Operational User site (OU) site, a Regional/Service Center (R/SC) and a Remote User (RU) site.

- The OU site represents an unclassified sensitive, system-high, local or regional site, or, alternatively may be an unclassified sensitive site with "Community of Interest" capability (COI site) incorporated. The COI case represents a mixed environment of users with varying privileges.
- The R/SC provides an interface between the Navy supported intranet and a public internet as well as the capability to perform additional security filtering and switching between dissimilar security infrastructures.
- The RU site supports travelling user or remote administrator's requirements for access to their applications normally provided at their home OU site.

The following discussion of the Navy system configurations will focus on privileges of people, sensitivity of data, administrative control, physical protections, and network connections that the TOE must exhibit in each of these configurations. Once user requirements and corresponding data flows for each site are understood, the protection requirements necessary for each site will be identified.

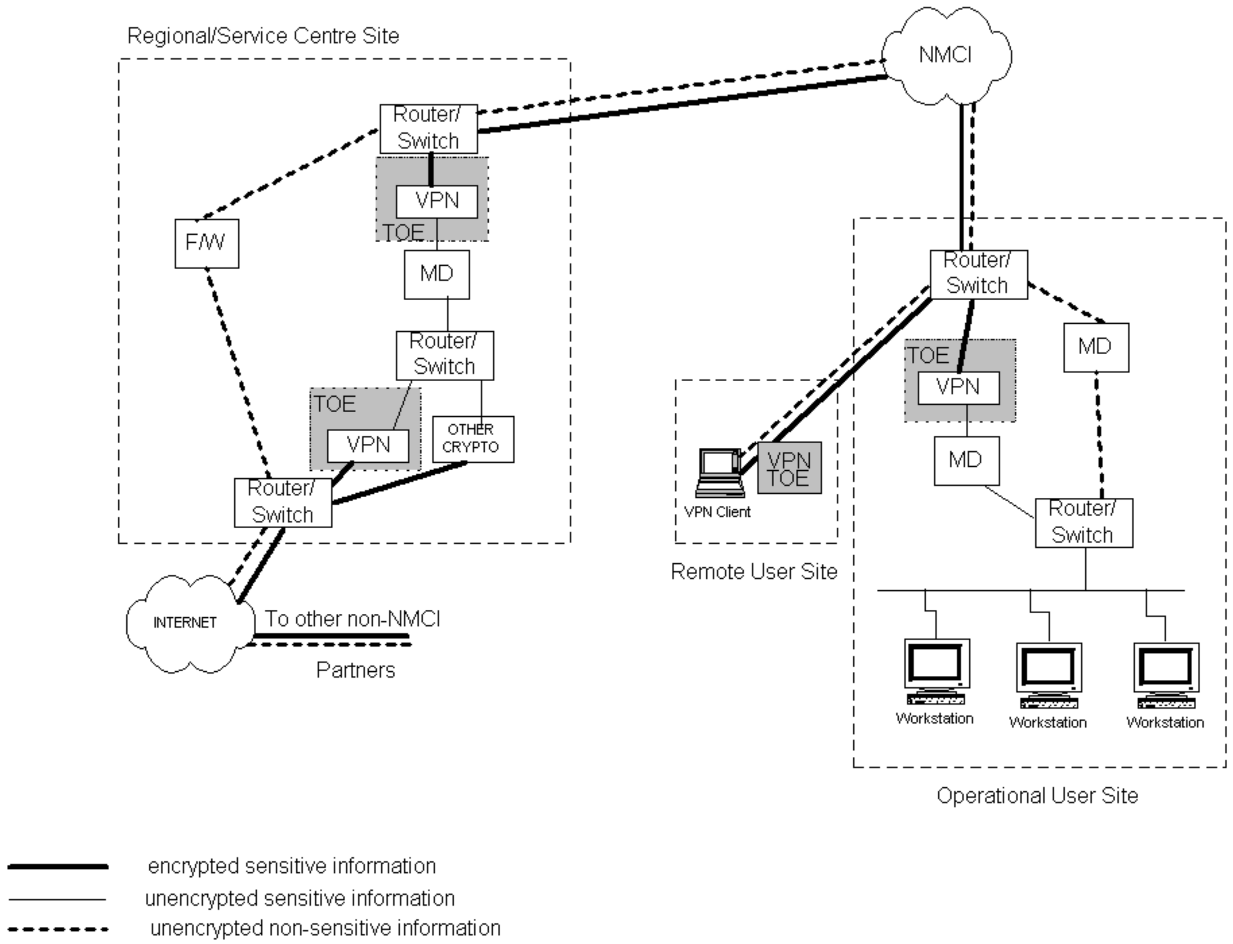

Figure 2 Navy VPN Generic Sites

2.3.1 The Operational User (OU) Site

The OU site is within a controlled facility and is closely analogous to "traditional" IT security environments (e.g. an unclassified, sensitive, system-high enclave). These sites are physically protected, with access limited to Authorized Users and authorized System and Security Administrators. Site administration is provided by clearly identified, well trained (typically resident), authorized System and Security Administrators.

An OU site may either be a single physical facility (e.g. individual office, a single building, or ship) or a distributed facility which is still considered as a single system-high enclave (e.g. military base, corporate campus facility) assuming security protection exists for the information flowing between the facilities. An OU site is considered to be under the command of a clearly identified senior official. This official establishes local site security policy (which the Information Security Officer normally writes) and appoints authorized System and Security Administrators, who will interpret and execute that policy and insure that the OU site security mechanisms enforce it. Typically, information contained within an OU site is related to only personnel whose mission and functions are directly related to that site and are subject to the supervision (either directly or indirectly) of the same senior official.

Authorized Users (AUs) within both the localized and distributed OU sites have the same basic requirements for connectivity and, therefore, no distinction is made between these configurations in this protection profile.

In many OU sites, because all AUs are approved for access to information (system-high), robust protection within the site is not normally required. When leaving or entering these sites via a shared network, AU's communications traverse through adequate boundary protection mechanisms that are capable of enforcing the site's security policy. As an example, one such policy could be that packets with certain destination IP addresses are encrypted via the VPN mechanism, while others bypass the VPN and are not encrypted.

We have described a military example above. We observe that OU sites are prevalent in almost all situations, public and private.

An OU site with COI (Community of Interest) capability is similar to the pure unclassified sensitive OU site (see Figure 3). The distinction is that it provides more granular data segregation (confidentiality and integrity protection) in support of Authorized User (AU) requirements. This involves the sharing of information with a subset of COI AUs who have "like privileges" and who also have the need to exclude other AUs and Unauthorized Agents who, by policy, don't have "need-to-know" authorization to share the COI related data. Members of a COI have common authorizations and require privacy enforcement to segregate their data from lesser-privileged users. Examples of COIs are engineering groups, research groups, specific project personnel, personnel officers, and payroll division, who may all be members of a single unclassified sensitive OU site (or multiple OU sites) while still having a requirement to segregate their privileged data from persons outside their group. More than one COI can be located within an OU site. Between COI users located in separated sites, user's communications traverse through adequate boundary protection mechanisms that are capable of enforcing the site's security policy. Within this protection profile we have proposed that client based VPN technology is suitable for providing COI protection

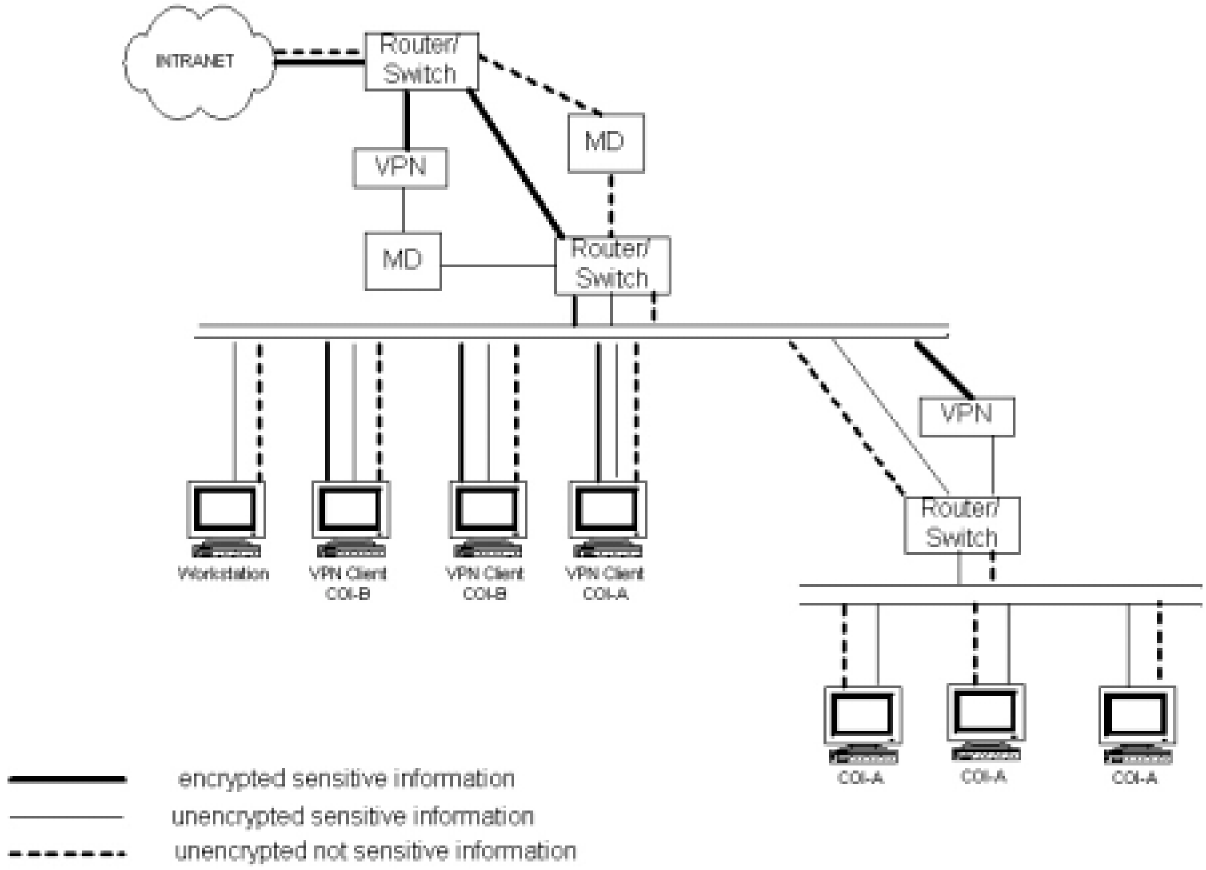

Figure 3 Community of Interest (COI) Site

2.3.2 Regional/Service Center (R/SC)

The R/SC site depicted in Figure 2 represents the Navy's communications infrastructure site. The Navy is planning to have several of these sites deployed worldwide which will segregate Navy intranets from internet connections. The R/SC will perform two basic functions:

- Communications: The R/SC site is the interface between groups of OU sites and the Internet.

- Security services in accordance with the Navy's Security-in-Depth philosophy. One such service is to provide communication service between dissimilar infrastructures, such as algorithm translation between dissimilar security infrastructures. Another is to support "Misuse Detection" (MD) (see definition in Terminology section) for all communications flowing through it.

The R/SC can be represented as two mirror image OU sites. Between the back-to-back VPN TOE the communication path is decrypted allowing analysis of the plain text by the MD system. For the purpose of defining the VPN TOE, this site is logically equivalent to the functionality of the OU site. Therefore, we have chosen to discuss the TOE in the context of the OU site, (TOE_{OU}) rather than as a unique R/SC site TOE.

2.3.3 Remote User (RU) Site

The RU site is a computer operated by an AU or System or Security Administrator who is "on the road." The RU site is external to a controlled facility though closely associated with a "home" site. Physical protection is typically limited and is usually compared to the protection provided to "high-valued" equipment or assets such as a personal computer. AUs of an RU site are required to take precautions commensurate with the handling of unclassified sensitive information during periods of operation of the RU site. In addition, they will be responsible for implementing adequate protective mechanisms during periods of non-operation. The associated home site's System and Security Administrators implement and administer RU site security policy. However, the Authorized User of the RU site is required to adhere to policy driven procedures on a day-to-day basis without the direct supervision or monitoring of the System or Security Administrator. Information processed by the RU is limited to unclassified sensitive data, and the user's privileges are limited to those he would have if resident at his home site. Travelling users, telecommuters and other select entities such as System or Security Administrators performing remote administration functions are all treated as RU Authorized Users in this profile. A key difference between a RU site and its associated home site is the lack of physically large or expensive infrastructure elements or security mechanisms such as dedicated boundary protection devices or administrator monitored MD systems that are more often associated with a multi-user facility such as the OU site**.**

Typically, a remote user accesses his associated home site either indirectly via a modem and an Internet Service Provider (ISP), or via a direct Internet connection. A unique problem associated with this user accessing his home site is that he has no knowledge regarding the sensitivity of files until he has actually accessed them. For instance, a remote user requesting access to his associated home site mail server account may not have prior knowledge of the sensitivity of individual mail files until after he has retrieved them. Associates who send e-mail to fellow home-site users within the same site and are not aware that the intended recipient is located remotely compound this problem. Therefore, they are not aware of the need to apply security mechanisms appropriate for release of the data external to their shared environment.

Consequently, we strongly recommend that ALL RU site accesses require robust protection when accessing a sensitive OU site. Thus, we recommend confidentiality, source authentication and integrity protection for all traffic to and from the RU site. We recommend this even in the case where the user is reasonably sure that he will not expose sensitive data.

3. TOE Security Environments (TSE)

As previously explained for the purpose of this PP the TOE will focus on the VPN functionality contained within a larger TOE Security Environment (TSE). Within the entire TSE, security-related functionality is provided beyond the scope of the VPN technology and includes functionality such as firewall filtering/boundary protection, MD, source routing, and virus scanning. This PP will not examine this additional security functionality which must be provided by the TSE in support of the defined TOE.

Figure 4 depicts two typical TSEs that generalize user's requirements for protection of unclassified sensitive data as it moves between unclassified sensitive system-high environments across shared networks. These typical TSEs support the previously described Navy configurations as well as most private sector applications of VPN technology.

Due to factors such as affordability, physical security protection, and mobility requirements, we have depicted two types of TOEs one, supporting multi-user sites (TOE_{OU}) (which includes the Navy's OU, COI and R/SC site configurations) and a second supporting remote user (RU) sites (TOE_{RU}).

The physical environments in which these two different TOEs and associated TSEs reside also differs, and consequently there is a need to consider applicable threat, site security policy, assumptions and security objectives for each TSE separately as well.

Note that the OU site provides physical and logical separation between the boundary security functions (which includes the TOE_{OU}) and other site components, while at the RU site the physical environment includes both the security and non-security related functions. In addition, the TOE_{RU} is typically hosted on the same component or computing platform (refer to figure 4). In the OU site, all the users share the boundary security components. Resident System and Security Administrators provide system and security administration. AUs located at an OU site will not have either physical access to boundary security components or logical access to administrative functions. In the RU site however, the physical security boundary is not differentiated from the entire TSE. The AU of the RU site has physical access to the TOE_{RU} and all other security-related components contained within the TSE. The RU site AU performs day-to-day procedures supporting non-resident administration as directed by his associated home site's System and Security Administrators.

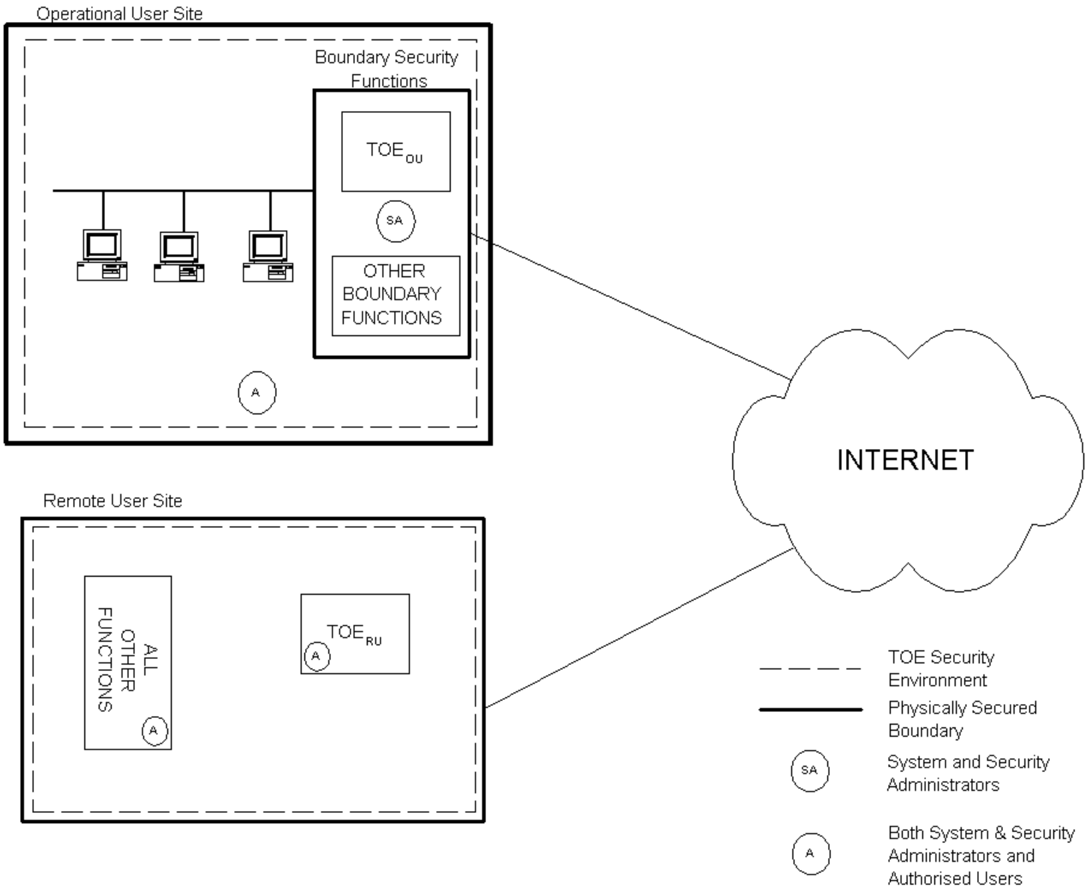
Operational User Site
Boundary Security Functions
TOE OU
SA
OTHER BOUNDARY FUNCTIONS
A
INTERNET
Remote User Site
ALL OTHER FUNCTIONS
A
TOE RU
A
TOE Security Environment
Physically Secured Boundary
SA
System and Security Administrators
A
Both System & Security Administrators and Authorised Users

Figure 4 TOE Security Environments

The TSE is further described in terms of associated threats, policies and assumptions. The itemized threats and policies resulted from our security analysis and are relevant to either, the TOE$_{OU}$, the TOE$_{RU,}$ or, the TSE in each of these environments. Assumptions relate to either the TOE$_{OU}$, the TOE$_{RU}$ or remainder of the TSE in each of these environments. Assumptions serve to establish the context relative to the allocation of security objectives to the VPN TOE$_{OU}$, VPN TOE$_{RU}$ or their supporting TSE.

Assumptions may provide information about the:

- *intended use of the TOE, including such aspects as the intended application, potential asset value, and possible limitations of use; and/or*
- *TSE including physical, personnel, and connectivity issues.*

Assumptions will:

- *mitigate threats to the TOE and, thus, eliminate TOE Objectives by assigning Objectives to the associated TSE; or*

- *generate specific TOE objectives in each environment.*

3.1 Threats to Security

The following threats to a site's assets are those threats that our security analysis found to be relevant to the entire TSE (including associated TOEs) at both the OU site and the RU site. The total list of threats is, in general, applicable to both the OU and RU implementations.

Sometimes, the degree to which specific threats threaten the information or resources at either the OU or RU site configurations differs. These differences in threat to each of the site configurations will often result in differing security assumptions (section 3.3), security objectives (section 4) and security requirements (section 5)

T.ATTACK_DATA - The TOE will encounter data that may contain malicious code. An Authorized User or Unauthorized Agent may use malicious code to attempt to disrupt site security operations or the TOE itself.

T.BAD_ACCESS_INAPPROPRIATE - Authorized Users may intentionally or unintentionally access or modify information, utilize resources for which they are not approved, or release sensitive data to unprivileged parties.

T.BAD_ACCESS_UNAUTHORISED - Unauthorized Agents may intentionally access or modify information, or utilize resources for which they are not approved.

T.BAD_ADMIN_ERROR - System or Security Administrators may unintentionally make a security relevant error that results in inappropriate access or modification of information, or inappropriate utilization of resources.

T.BAD_ADMIN_HOSTILE - The System or Security Administrator intentionally takes a security relevant action that results in inappropriate access or modification of information, or inappropriate utilization of resources.

T.BAD_AUDIT_OVERFLOW - Legitimate audit records may be lost due to excessive volume of records.

T.BAD_AUDIT_SEQUENCE - Legitimate audit records may not be attributed to time of occurrence resulting in audit analysis that is inconclusive.

T.BAD_AUDIT_UNDETECTED - Intentional or unintentional access or modification of information or utilization of resources may go undetected whether performed by Authorized Users, System or Security Administrators or Unauthorized Agents.

T.BAD_AUDIT_UNTRACEABLE - Access to, or modification of information, or utilization of resources by Unauthorized Agents may not be traceable to their source.

T.BAD_DESIGN_BYPASS - The design or architecture of the system allows security mechanisms to be bypassed and this bypass function (typically used to communicate with lessor privileged users) may be inappropriately utilized. Either the bypass technique or function may be embedded within the TOE (e.g. RU site TOE) or external to it located within a shared boundary security functional area (e.g. OU site Boundary Security Function).

T.BAD_DESIGN_COMPLEXITY - Authorized Users, System or Security Administrators, may accidentally modify security functions, because of the complexity of the design or operation resulting in a violation of the site security policy.

T.BAD_DESIGN_EXTERNAL - System design is insufficient to prevent random conditions external to the TSE from resulting in detrimental affects. Examples are lightening storms and human error.

T.BAD_DESIGN_SECURITY_FUNCTION_CORRUPTION - System design is insufficient to prevent Unauthorized Agents from modifying security critical functions within the TSE.

T.BAD_PROCEDURES - Operational procedures are either inadequate or are not followed, resulting in unapproved access or modification of information, or inappropriate utilization of resources. Examples are: Storage media is allowed to age rendering it unreadable; Virus checking capability is insufficient resulting in loss or compromise of data; Inadequate TOE configuration data back up procedures or mechanisms result in the inability to restore the TOE to normal operation.

T.COVERT_CHANNELS - An Authorized User, System or Security Administrator may intentionally or unintentionally transmit via a covert channel sensitive information to Unauthorized Agents who are not privileged to see it.

T.CRYPTANALYTIC – Unauthorized Agents may passively attack the cryptography of the TOE using cryptanalytic methods.

T.MALFUNCTION - Failures occur in ways that result in inappropriate access or modification of information, or inappropriate utilization of resources.

T.MASQUERADE_BYPASS - An Unauthorized Agent may bypass identification and authorization mechanisms in order to access or modify information, or utilize system resources. Attack strategies include password guessing, password stealing, password sniffing, all followed by replay, and IP address spoofing.

T.MASQUERADE_HIJACK - An Unauthorized Agent may intrude on a properly established session in order to access or modify information, or utilize system resources.

T.MULTIPLE_PATHS - More than one path may exist for data to flow in and out of sites and may consequently bypass intended security functions.

T.PHYSICAL_SECURITY – Physical security of the TSE may be inadequate to either deny UA access to information which is processed or stored within the TSE, or deny the use of (or integrity of) TOE resources. Because RU sites typically are located in higher threat environments with only a single user monitoring physical security, this threat may be more significant for RU sites.

T.POLICY_INTERPRETATION - Site Information Security Officers may not interpret organizational security policy consistently or correctly. This could result in a violation of the intended security policy when one site interprets and implements a policy differently from another site.

T.REPUDIATION - Authorized Users or Systems or Security Administrators may deny originating or receiving data transfers or performing malicious acts.

T.TEMPEST Unauthorized Agents may receive sensitive data, which has radiated or is conducted from the TOE.

T.TRAFFIC_ANALYSIS - Identification of Authorized Users or other sensitive information may be deduced by observing the TSE or related resources (e.g., plain text source/destination addresses, traffic volume, and human response or actions.)

T.TRANSMISSION_ERRORS - Transmission errors can cause loss of data or data integrity.

T.UNAVAILABLE - The Internet, PSTN, or shared public network may be unavailable.

3.2 Site Security Policy

The following policy statements identify and explain organizational policy or rules which are relevant for the TSE (including associated TOE) at both the OU site and the RU site. Frequently, organizational policy implemented will differ between OU sites and RU sites. These differences will be reflected in slight modifications to associated assumptions (section 3.3) or objectives (section 4) applicable to each site. Likewise, there may be differences in security requirements (section 5) for each applicable TOE (e.g. $\mathrm{TOE}_{\mathrm{OU}}$ or $\mathrm{TOE}_{\mathrm{RU}}$).

P.ACCOUNT Authorized Users, System and Security Administrators must be held accountable for security relevant actions

P.ADMIN_SECURITY_RESTRICTED - Only Authorized System and Security Administrators and trained maintainers may administer or repair security mechanisms in their assigned site TSE. At RU sites, limited on-site administration will be performed by the RU, but only as authorized and directed by their associated home OU site, System and Security Administrator.

P.AUDIT_REVIEW - Audit data will be reviewed, analyzed, and as appropriate, acted upon.

P.AVAILABLE - Access to communications such as the Internet, PSTN or other public network connections will be available to Authorized Users when required. An Information Security Officer will develop policy governing the use of these communications and the System and Security Administrators will implement this policy.

P.COMPLY The implementation and use of the organization’s IT systems must comply with all applicable laws, regulations, and contractual agreements imposed on the organization.

P.DEFEND The TOE shall defend itself from improper operation caused by attacks via the communications channels.

P.DISTRIBUTION - Control of the issuing of security relevant TOE hardware, software and all other resources will be maintained.

P.DUE_CARE The organization’s IT systems must be implemented, maintained and operated in a manner that represents due care and diligence with respect to risks to the organization. The level of security afforded the IT system must be in accordance with what is considered prudent by the organization’s or system’s accrediting authority.

P.LABEL All unclassified sensitive or COI information will be appropriately identified regardless of physical or electronic representation.

P.MANAGE The TOE shall be managed and maintained such that its security functions are implemented and preserved throughout its operational lifetime.

P.PERSONNEL_TRUST_COI **-** All Authorized Users, System and Security Administrators and maintainers of TOE resources, which process COI information or Authorized Users of COI information, will be granted privileges for their specific COI privilege level.

P.PERSONNEL_TRUST_MINIMUM **-** All Authorized Users, System and Security Administrators and maintainers of TOE resources will possess a minimum sensitive privilege level.

P. PROCEDURES **-** Procedures will be in place to restrict inadvertent disclosure or modification of sensitive information or improper utilization of resources in the TSE. Examples: Printed material handling procedures, procedures to lock computers when unattended, and guidelines for proper disposal of media.

P.PROTECT - Confidentiality and integrity protection must be applied to sensitive information before it leaves the TSE to a network servicing less privileged users.

P.RECIPIENTS - Communications through the TOE shall only be between Authorized Users or System and Security Administrators.

P.RELEASE_NON-SENSITIVE **-** All non-sensitive information in a sensitive or COI environment is implicitly marked “Sensitive” or “COI” respectively. Information in these environments must be reviewed or filtered before releasing it unprotected outside the TSE.

P.REMOTE_SECURITY_ADMIN - Authorized System and Security Administrators may remotely administer devices in the TSE through protected external communication channels

P.TOE_USAGE – TOE usage, and the ability to release data from a TOE, will be limited to personnel who have been properly authenticated and deemed to be Authorized Users, System or Security Administrators. Remote User (RU) privileges, and usage of a TOE from a remote location, will be tightly controlled and procedurally limited to situations where there is a strong operational requirement.

P.TRAIN All Authorized Users, Systems and Security Administrators and maintainers of TOE resources will be properly trained to the level of their responsibility.

P.TSE_CONNECTIONS **-** All connections between the TSE and external networks will be controlled. At an OU site these connections will be made through boundary protection functions which are physically isolated and accessible by only the System or Security Administrators. At a remote site, connections between the TSE and the network will be established by the RU and boundary protection functionality will be under the direction and procedural control of the RU**.**

P.USAGE The organization’s IT resources must be used only for authorized purposes.

.

3.3 Secure Usage Assumptions

Assumptions will describe the security aspects of the environments in which the OU site TOE and the RU site TOE will be used. Assumptions will include the following:

- *Information about the intended use of the TOE, including such aspects as the intended application, potential asset value, and possible limitations of use; and*
- *Information about the TOE's environment including physical, personnel, and connectivity issues.*

The list of assumptions has been broken down into three subsections. Subsection 3.3.1 itemizes assumptions (formatted as "A.<descriptive assumption name>") which are applicable to the TSEs associated with ***both*** the OU and RU sites. Subsection 3.3.2 itemizes assumptions (formatted as "A_{OU}.<descriptive assumption name>") which is applicable to the TSE associated ***only*** with the OU sites. Subsection 3.3.3 itemizes assumptions (formatted as "A_{RU}.<descriptive assumption name>") which is applicable to the TSE associated ***only*** with the RU sites.

3.3.1 OU and RU Site, Secure Usage Assumptions

A.ADMIN At an OU site there are resident system and security administrators. They have a vital role in the organization and are given much trust. However, occasionally they may prove themselves untrustworthy. Restrictions should exist to limit their ability to effect unwanted changes to the TSE security functionality.

OU site administrative responsibilities will be split between a system administrator and a security administrator who together will be able to administer the entire system. The assignment of split administrative authorization is established in order to prevent unrestricted system control and to provide for "checks and balances."

TOE_{RU}s will be initially configured by the user's associated home OU site administrator(s). However, limited day-to-day administration of the TOE_{RU} will be performed by the authorized remote user under the direction of the associated system or security administrator.

A.AVAILABLE Internet, PSTN or other required public network connections are available to the TSE when required.

A.BACK_UP Back ups of TOE files and configuration parameters are performed in accordance with site security policy as required. They are sufficient to restore TOE operation in the event of a failure or security compromise. Back ups are transparent to the user and performed automatically on a timely basis as determined by site policy.

A.CRYPTANALYTIC – Cryptographic methods used in the TOE will be resistant to cryptanalytic attacks and be of adequate strength to protect sensitive data.

This assumption makes no statement about the robustness of the implementation of these cryptographic methods.

A.CRYPTO_SUPPORT - Cryptographic support infrastructure will be provided by procedures and mechanisms external to the TOE. Examples: user registration, key issuance, directory services, and assignment of privileges.

A.DESIGN_BYPASS - Any bypass of the TOE will be performed outside the TOE but within the TSE. At an OU site, bypass functions will be performed within a physically controlled boundary protection area, which is accessible to only System and Security Administrators. At an RU site, bypass functions, if required, will be performed utilizing periods processing techniques.

A.INFO_SECURITY_OFFICER - An Information Security Officer is responsible for creating, maintaining, interpreting and overseeing consistent implementation of site security policy and procedures.

A.MISUSE_DETECT – Misuse Detection (MD) mechanisms exist outside of the TOE that look for potential misuse (e.g. unauthorized access, unusual modification of information, virus scanning, or unexpected utilization of resources). The MD mechanisms include tools for audit reduction and analysis which will be used to actively scrutinize the system and network for irregularities and provide notification to appropriate authorities for follow up action.

A.POLICY_COMPLIANCE - System and Security Administrators and Authorized Users of the TOE will typically do their best to competently and accurately carry out established site security policy.

A.LOGISTICS_SUPPORT – Logistics support planning will be completed and implemented to ensure that sufficient spare parts are available to quickly restore service to the TSE when failures occur.

A.TEMPEST The TOE is designed adequately such that the risk of sensitive data emanating from the TOE is minimal. No specific DoD TEMPEST design or test requirements will be levied on the TOE.

A.THREAT_LEVEL – The threat agent is somewhat sophisticated, has minimal though adequate resources, and is willing to take moderate risk.

A.TRAIN All Authorized Users, System and Security Administrators, and maintainers are appropriately trained.

A.USER_TRUSTED - Authorized Users of the TSE are trusted. However, occasionally they may prove themselves to be untrustworthy.

3.3.2 OU Site, Secure Usage Assumptions (A_{OU})

A_{OU}.PHYSICAL_SECURITY - Physical security of the TSE at an OU Site is adequate to protect unclassified sensitive and unclassified sensitive/COI information and resources. At an OU site, the TOE_{OU} will be located within a physically controlled boundary protection area which is accessible to only the System and Security Administrators.

3.3.3 RU Site, Secure Usage Assumptions (A_{RU})

A_{RU}.PHYSICAL_SECURITY - Physical security of the TSE at an RU Site must be considered limited since remote sites are typically located in a higher threat environment. The TOE_{RU} is normally under the supervision of a single individual and may occasionally be left unattended. In addition, the TOE associated with a RU may even be accessed by unauthorized agents (i.e. security inspections at airports, maids in hotels, etc.).

4. Security Objectives

The section will itemize the security objectives for the TOE_{OU}, the TOE_{RU}, and the TOE Security Environments associated with each TOE. These security objectives will address all aspects of the security environment identified. The security objectives will reflect the stated intent of the applicable TOE or TSE, and will be suitable to counter all identified threats and cover all identified site security policy and assumptions. The itemized security objectives will be categorized as either security objectives for both type TOEs (itemized in section 4.1.1), the OU TOE (O_{OU}) (section 4.1.2), the RU TOE (O_{RU}) (section 4.1.3) or security objectives for the associated TSEs (O_{TSE}) (sections 4.2.1, 4.2.2 and 4.2.3).

Security objectives for the TOE_{OU} and TOE_{RU} will be clearly stated and traced back to aspects of identified threats to be countered by the OU and RU TOEs and/or site security policy to be met by the OU and RU TOEs. Security objectives for the environment will be clearly stated and traced back to aspects of identified threats not completely countered by the OU and RU TOEs and/or site security policy or assumptions not completely met by the OU and RU TOEs.

4.1 TOE Security Objectives

4.1.1 Security Objectives for Both the OU and RU Site TOEs

O.ADMIN The TOE must provide functions to enable System and Security Administrators to effectively manage and maintain the TOE and its security functions, ensuring that only they can access administrative functionality. This objective extends to remote users who are functioning as the administrator at the RU site.

O.ADMIN_INTERFACE - The TOE must have a friendly set of human interfaces to maximize error free administration.

O.ADMIN_SECURITY_REMOTE - The TOE needs to support a secure path capability (providing confidentiality, data integrity, and administrator authentication) to ensure remote administration is performed securely.

O.ADMIN_SEPARATE – Both the TOE_{OU} and the TOE_{RU} will support two administrative roles, System Administrator and Security Administrator. The Security Administrator will configure the TOE_{OU} and TOE_{RU} to implement these two separate roles as defined by the site security policy. In addition the Security Administrator will configure all associated RU site TOE_{RU} devices to allow for the authorized RU to perform limited administrative functions.

O.ALARM The TOE will be capable of detecting and responding to violations of the site security policy as related to the TOE operation. Violations that are detected either by the TOE or the MD system, which may be attributed to inappropriate operation of the TOE (internal TOE violations), will be reported to System and Security Administrators, and where appropriate, the AU of RU sites. Violations, which may be attributed to inappropriate operation or failures external to the

TOE, which are detected by the MD function (external violations) will also be reported to the same personnel. In either case, upon detection of either an internal or external violation or failure that cannot be automatically cleared the TOE will default to a secure state and suspend processing.

O.AUDIT The TOE must provide an audit record to notify an audit analysis tool of security relevant events such that Unauthorized Agents, Authorized Users, System and Security Administrators actions can be detected and potentially held accountable for their actions. The audit data must be easily understood and be protected from unauthorized modification. Audit events must be selectable.

O.BACK_UP The TOE must be capable of backing up designated files and configuration parameters automatically. The back up capability must be configurable, based on established site security policy, so that the back up capability could occur upon start-up, shutdown, or after specified periods of usage. The backed up files and parameters will be stored either within the TOE or within another device located within the TSE.

O.CONFIDENTIALITY - The TOE will provide confidentiality by protecting the content of information released from either the OU site or RU site destined to other equivalently privileged TOEs. Upon receipt of protected data, the recipient TOE will remove the confidentiality protection invoked by the transmitting TOE.

O.CONNECT Connectivity will be provided only between peer TOEs upon the request of Authorized Users who have been properly identified to their associated TOE. Upon establishment of a TOE-to-TOE connection, the initiating TOE will notify the associated client host equipment that a VPN tunnel has been established.

O.CRYPTO_SUPPORT - The TOE must interface with cryptographic support mechanisms, which establish files and configuration parameters and insure the integrity of these files and parameters. File examples are: Authorized User registration data, key issuance and revocation lists, access control lists, and assignment of AU privileges files.

O.HALT The TOE will stop processing data and default to a secure state whenever a failure or insecure operations are detected.

O.INTEGRITY The TOE will apply integrity protection to all information it releases to a peer TOE. Upon receipt of protected data, the TOE will verify that the received data accurately represents the data that was protected.

O.PROPER_SPEC - The TOE will provide adequately strong security protections to counter the various ways an attack may occur (e.g. The strength of cryptographic algorithms, the length of key, and the design of access control lists must be appropriate for sensitive data and operations.)

O.PROTECT_ADDRESSES - The TOE_{OU} will protect the confidentiality and integrity of the transmitting and receiving Authorized User's addresses. Upon receipt, the TOE will correctly interpret both originating and destination Authorized User's addresses.

O.RELIABLE - The TOE will be reliable with a predicted availability of .97 ("minimal delay" as required for "Mission Support" operations) when operated in a typical office environment.

O.REPLAY_PREVENT - The TOE will prevent access to the TOE and TSE resources from Unauthorized Agents who attempt a replay attack through the TOE by masquerading as an Authorized User.

O.SECURE_STARTUP - Upon initial start-up of the TOE or recovery from an interruption in TOE service, the TOE must default to a secure state and not compromise its files, configuration parameters, or information being processed before the interruption occurred.

O.SECURITY_FUNCTION - Authorized User's control over TOE security functions will be kept to a minimum.

O.SELF_TEST The TOE will perform self-tests of its security functions including those required by the site security policy and site procedures.

O.SEPARATION - The TOE will ensure that residual information from one session does not spill over to another.

O.TOE_AVAILABLE - The TOE will be resilient to denial-of-service attacks.

O.TOE_USER_ASSOCIATION - The TOE must include a mechanism, which associates all Authorized Users with their assigned site and associated TOE. This mechanism will allow properly identified and authenticated transmitting users to designate only the desired recipient. Based on this mechanism the transmitting TOE will either allow or reject connectivity.

4.1.2 Security Objectives for the OU Site TOE (O_{OU})

O_{OU}.IDENTIFY_USER - Usage of the TOE_{OU} will be continuously restricted to only properly identified Authorized Users, and System or Security Administrators. Identification of Authorized Users may minimally be based on an asserted IP address and correct password. Identification of System or Security Administrators will be based on the use of hardware tokens.

O_{OU}.SPECIAL_PURPOSE - The TOE_{OU} is a Special Purpose Device (definition previously provided in Terminology section) and consequently will not execute general-purpose programs.

4.1.3 Security Objectives for the RU Site TOE (O_{RU})

O_{RU}.IDENTIFY_USER - Usage of the TOE_{RU} will be continuously restricted to only properly identified Remote Users, and System or Security Administrators. Identification of Remote Users and System or Security Administrators will be based on the use of hardware tokens.

4.2 Security Objectives for the TOE Security Environments

4.2.1 Security Objectives for both the OU and RU, TOE Security Environments

OE.ADMIN - Competent System and Security Administrators will be assigned as required.

OE. ALARM – Within the TSE there will be a mechanism to alert System and Security Administrators, (or at an RU site, AUs) to alarm conditions.

OE.AUDIT The TSE must provide the capability to store and analyze recorded security relevant events as well as a means to search and sort the audit trail based on relevant attributes.

OE.BACK_UP Devices other than the TOE, contained within the TSE, which affect the secure operation or availability of the TOE functionality, must have the capability to store back up files and configuration parameters which are necessary to restore the TOE functionality following an interruption or malfunction of the system.

OE.CONNECT At an OU site connectivity between Authorized Users who do not have equivalent privileges will be regulated by other devices external to the TOE_{OU} but within the TSE. At an RU site, the AU must use periods processing techniques such as, replacement of hard drives, zeroization of active memory, frequent virus checking, or equivalent techniques whenever connectivity is initiated between AUs who do not have equivalent privileges.

OE.CRYPTO_SUPPORT – Necessary cryptographic support infrastructure will be available and sufficient to support services such as, user registration, key issuance, key destruction, directory services and assignment of privileges.

OE.HALT Mechanisms within the TSE will be capable of sending a command to the TOE which will inhibit its operation.

OE.INFO_SECURITY_OFFICER – An Information Security Officer will be identified who will be responsible for creating, maintaining, interpreting and overseeing consistent implementation of site security policy and procedures.

OE.LOGISTICS_SUPPORT – Logistics planning and support will be completed and validated in order to assure specified availability requirements.

OE.MISUSE_DETECT - A capability that exists in the TSE and consists of automatic, semi-automatic and static tools that are used by the system itself and its administrators to check on the secure operation of the organization’s IT resources. The organization’s Information Security Officer will develop policy for proper use of these tools and mechanisms. The administrators and AUs will be trained in the proper use of the tools and mechanisms and will be charged with appropriately implementing policy regarding them. Tools and mechanisms within this package called MD include virus scanning, network mapping, sniffers, auditing, and analysis.

OE.PERSONNEL - The organization will make every attempt to hire and maintain trustworthy and competent personnel. Some available methods are testing, security lectures, polygraphing, peer monitoring, and Misuse Detection analysis.

OE.REVIEW Authorized System and Security Administrators will periodically review audit trail information.

OE.SECURITY_FUNCTION - Authorized User's control over TSE security functions will be kept to a minimum.

OE.TOE_MANAGE - The TOE will be delivered, installed, configured, maintained and operated in a manner consistent with the established site security policy.

OE.TRAIN The organization will make every attempt to ensure that Authorized Users and System and Security Administrators are adequately trained to the level of their responsibility.

4.2.2 Security Objectives for the OU, TOE Security Environment (OE_{OU})

OE_{OU}.CONNECTION_MAPPING – At an OU site the TSE will include the ability to map network and modem connections in order to detect unauthorized connections.

OE_{OU}.PHYSICAL_SECURITY - The TOE_{OU} will be protected within the Operational User Site in order to limit physical access to authorized System and Security Administrators in accordance with FIPS 140-1, Level 2.

4.2.3 Security Objectives for the RU, TOE Security Environment (OE_{RU})

OE_{RU}.PHYSICAL_SECURITY – Physical security of the RU site will be sufficient to protect the sensitive data during both operational and inactive periods. When the TOE_{RU} is left unattended procedures such as media encryption or secure storage of the hard drive, will be used to insure the protection of stored data. In addition, during periods when the TOE_{RU} is not being used, the hardware token will be removed and under the protection of the AU.

5. IT Security Requirements

This section provides functional and assurance requirements that must be satisfied by a Protection Profile-compliant TOE. These requirements consist of functional components from Part 2 of the CC and an Evaluation Assurance Level (EAL) containing assurance components from Part 3 of the CC.

5.1 TOE$_{OU}$ Security Functional Requirements

The functional security requirements for the TOE$_{OU}$ consist of the following components derived from Part 2 of the CC and are summarised in Table 2.

Table 2 TOE$_{OU}$ Functional Security Requirements Summary

Requirement Class	Requirement Family	Requirement Component
FAU – Security Audit	ARP – Security Alarm	.1 Security Alarm
	GEN – Security Audit Generation	.1 Audit Data Generation
		.2 User Identity Association
	SAR – Security Audit Review	.1 Audit Review
		.2 Restricted Audit Review
	SEL – Selective Audit	.1 Selective Audit
FCO - Communication	None	None
FCS – Cryptographic Support	CKM – Cryptographic Key Management	.1 Crypto Key Generation
		.2 Crypto Key Distribution
		.4 Crypto Key Destruction
	COP – Cryptographic Operation	.1 Cryptographic Operation
FDP – User Data Protection	ACC- Access Control Policy	.2 Complete Access Control
	ACF – Access Control Functions	.1 Security Attribute Based Access Control

(continued) FDP – User Data Protection	ETC – Export of User Data w/o Security Attributes	.1 Export of User Data w/o Security Attributes
		.2 Export of User Data with Security Attributes
	ITC – Import of User Data with Security Attributes	.2 Import of User Data with Security Attributes
	RIP – Residual Information Protection	.2 Full Residual Info Protection
FIA – Identification & Authentication	AFL – Authentication Failures	.1 Authentication Failure Handling
	ATD – User Attribute Definition	.1 User Attribute Definition
	SOS – Specification of Secrets	.1 Verification of Secrets
		.2 TSF Generation of Secrets
	UAU – User Authentication	.2 User Authentication Before any Action
		.3 Unforgeable Authentication
		.5 Multiple Authentication Mechanisms
		.6 Re-authenticating
	UID – User Identification	.2 User ID Before any Action
	USB – User-subject Binding	.1 User-subject Binding

FMT – Security Management	MOF – Management of Functions in TSF	.1 Management of Security Functions Behaviour
	MSA – Management of Security Attributes	.1 Management of Security Attributes
		.2 Secure Security Attributes
		.3 Static Attribute Initialisation
	MTD – Management of TSF Data	.1 Management of TSF Data
		.2 Management of Limits on TSF Data
		.3 Secure TSF Data
	SMR – Security Management Roles	.2 Restrictions on Security Roles
		.3 Assuming Roles
FPR – Privacy	ANO - Anonymity	.1 Anonymity
	UNO - Observability	.4 Authorised User Observability
FPT – Protection of TOE Security Functions	AMT – Underlying Abstract Machine Test	.1 Abstract Machine Test
	FLS – Fail Safe	.1 Failure with Preservation of Secure Path
	ITI – Integrity of Exported TSF Data	.1 Inter-TSF Detection of Modification
	PHP – TSF Physical Protection	.1 Passive Detection of Physical Attack
	RCV – Trusted Recovery	.2 Automatic Recovery
	RPL – Replay Detection	.1 Replay Detection
	RVM – Reference Mediation	.1 Non-bypassability
	SEP – Domain Separation	.1 TSF Domain Separation

FPT – (cont.) Protection of TOE Security Functions	STM – Time Stamps	.1 Reliable Time Stamps
	TDC – Inter-TSF TSF Data Consistency	.1 Inter-TSF Basic TSF Data Consistency
	TST – TSF Self Test	.1 TSF Testing
FRU – Resource Utilisation	FLT – Fault Tolerance	.1 Degraded Fault Tolerance
	RSA – Resource Allocation	.1 Maximum Quotas
FTA – TOE Access	LSA – Limitation on Scope of Selectable Attributes	.1 Limitation on Scope of Selectable Attributes
	MCS – Limitation on Multiple Concurrent Sessions	.1 Basic Limitation on Multiple Concurrent Sessions
	SSL – Session Locking	.3 TSF-Initiated Termination
	TSE – TOE Session Establishment	.1 TOE Session Establishment
FTP – Trusted Path/Channels	ITC – Inter-TSF Trusted Channel	.1 Inter-TSF Trusted Channel

Class FAU: Security Audit

FAU_ARP Security Audit Automatic Response

FAU_ARP.1 Security Alarms

FAU_ARP.1.1 The TSF shall take **action to: detect audit events, alert System and Security Administrators, generate and transmit audit records to an associated Misuse Detection System** upon detection of a potential security violation.

Dependencies:

FAU_SAA.1 Potential Violation Analysis

FAU_GEN Security Audit Data Generation

FAU_GEN.1 Audit Data Generation

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

1. Start-up and shutdown of the audit functions;
2. All auditable events for the *basic* level of audit; and
3. **The specifically detailed audit events listed in Appendix B.**

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

1. Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and
2. For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, **none.**

Dependencies:

FPT_STM.1 Reliable Time Stamps

FAU_GEN.2 User Identity Association

FAU_GEN.2.1 The TSF shall be able to associate each auditable event with the identity of the user that caused the event.

Dependencies:

FAU_GEN.1 Audit Data Generation

FIA_UID.1 Timing of Identification

FAU_SAR Security Audit Review

FAU_SAR.1 Audit Review

FAU_SAR.1.1 The TSF shall provide **both the System and Security Administrator and the Misuse Detection system** with the capability to read **all audit data** from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information**.**

Dependencies:

FAU_GEN.1 Audit Data Generation

FAU_SAR.2 Restricted Audit Review

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

Dependencies:

FAU_SAR.1 Audit Review

FAU_SEL Security Audit Event Selection

FAU_SEL.1 Selective Audit

FAU_SEL.1.1 The TSF shall be able to include or exclude auditable events from the set of audited events based on the following attributes:

1. ***specific file*** *identity, user identity*, ***specific process*** *identity, host identity, event type*

2. **time of day, date**

Dependencies:

FAU_GEN.1 Audit Data Generation

FMT_MTD.1 Management of TSF Data

Application Note: There is no intent to require the TOE to store audit records. What is required is the TOE must cryptographically protect the audit record before sending it to the Misuse Detection system for storage and analysis. Please note that FTP_ITC.1.3, Trusted Channels, supports this requirement.

Class FCS: Cryptographic Support

FCS_CKM Cryptographic Key Management

FCS_CKM.1 Cryptographic Key Generation

FCS_CKM.1.1 The TSF shall generate cryptographic key in accordance with a specified cryptographic key generation algorithm **pseudo-random number generation, Diffie Hellman exponents,** and specified cryptographic key sizes **equivalent to or greater than 112 bits of protection** that meets the following: **FIPS 140-2, Level 2**.

Dependencies:

[FCS_CKM.2 Cryptographic Key Distribution, or FCS_COP.1 Cryptographic Operation]

FCS_CKM.4 Cryptographic Destruction

FMT_MSA.2 Secure security attributes

FCS_CKM.2 Cryptographic Key Distribution

FCS_CKM.2.1 The TSF shall distribute cryptographic key in accordance with a specified cryptographic key distribution method **DoD medium assurance PKI for public key distribution using Class 4 X.509, version 3 certificates with hardware tokens for protection of private key used by System and Security Administrators** that meets the following: **DoD PKI Roadmap and ANSI X9.6**.

Dependencies:

[FDP_ITC.1 Import of User Data Without Security Attributes, or

FCS_CKM.1 Cryptographic Key Generation]

FCS_CKM4 Cryptographic Key Destruction

FMT_MSA.2 Secure Security Attributes

Application Note: This requirement mandates that hardware tokens (Class 4, X.509 version 3 certificates) be used by System and Security Administrators.

FCS_CKM.2 Cryptographic Key Distribution

FCS_CKM.2.1 The TSF shall distribute cryptographic key in accordance with a specified cryptographic key distribution method **DoD medium assurance PKI for public key distribution using Class 3 X.509, version 3 format for private key distribution in a software format** that meets the following: **DoD PKI Roadmap and ANSI X9.6**.

Dependencies:

[FDP_ITC.1 Import of User Data Without Security Attributes, or

FCS_CKM.1 Cryptographic Key Generation]

FCS_CKM4 Cryptographic Key Destruction

FMT_MSA.2 Secure Security Attributes

Application Note: This requirement mandates at least software tokens (Class 3, X.509 version 3 certificates) be assigned to all TOU$_{OU}$s.

FCS_CKM.4 Cryptographic Key Destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic key in accordance with a specified cryptographic key destruction method **zeroization of all plain text cryptographic keys and other critical security parameters within the device** that meets the following: **FIPS 140-2, Level 2**.

Dependencies:

[FDP_ITC.1 Import of User Data Without Security Attributes, or

FCS_CKM.1 Cryptographic Key Generation]

FMT_MSA.2 Secure security attributes

FCS_COP Cryptographic Operation

FCS_COP.1 Cryptographic Operation

FCS_COP.1.1 The TSF shall perform **data encryption services** in accordance with a specified cryptographic algorithm **3DES** and cryptographic key sizes **168 bits (equivalent to at least 112 bits of security protection) for 3DES** that meet the following: **Draft NIST FIPS Pub 46-3 for 3DES, Internet Engineering Task Force Request for Comment (RFC) 2401, "Security Architecture for the Internet Protocol," and RFC 2406, "IP Encapsulating Security Payload-Tunnel Mode**."

Dependencies:

[FDP_ITC.1 Import of User Data Without Security Attributes, or

FCS_CKM.1 Cryptographic Key Generation]

FCS_CKM.4 Cryptographic key destruction

FMT_MSA.2 Secure security attributes

Application Note: Future migration to incorporate the Advanced Encryption Standard (AES) is anticipated and will be approved when standards are established.

FCS_COP.11 The TSF shall perform **data source authentication and integrity protection** in accordance with a specified cryptographic algorithm **HMAC with SHA-1** and cryptographic key sizes **160 bits** that meet the following: **RFC 2104, "Keyed-Hashing for Message Authentication, dated February, 1997, and RFC 2404, "Use of HMAC-SHA-1-96 within ESP and AH".**

Dependencies:

[FDP_ITC.1 Import of User Data Without Security Attributes, or

FCS_CKM.1 Cryptographic Key Generation]

FCS_CKM.4 Cryptographic key destruction

FMT_MSA.2 Secure security attributes

Application Note: The Digital Signature Algorithm (DSA) is also acceptable and future migration to incorporate NIST approved Elliptic Curve DSA will be acceptable when standards are established.

FCS_COP.1.1 The TSF shall perform **hashing** in accordance with a specified cryptographic algorithm **Security Hash Algorithm 1 (SHA-1)** and cryptographic key sizes **160 bits** that meet the following: **FIPS 180-1**.

Dependencies:

[FDP_ITC.1 Import of User Data Without Security Attributes, or

FCS_CKM.1 Cryptographic Key Generation]

FCS_CKM.4 Cryptographic Key Destruction

FMT_MSA.2 Secure Security Attributes

FCS_COP.1.1 The TSF shall perform **key exchange** in accordance with a specified cryptographic algorithm **Diffie-Helman Algorithm** and cryptographic key sizes **at least 1024 bits** (**or NIST Elliptic Curves that provide equivalent or better strength)** that meet the following: **Internet Engineering Task Force, Request for Comment (RFC) 2401, "Security Architecture for the Internet Protocol"; and RFC 2409, "The Internet Key Exchange (IKE) using ESP," Tunnel Mode, Main Mode, Public Key Signatures.**

Dependencies:

[FDP_ITC.1 Import of user data without security attributes or

FCS_CKM.1 Cryptographic Key Generation]

FCS_CKM.4 Cryptographic Key Destruction

FMT_MSA.2 Secure Security Attributes

Class FDP: User Data Protection

FDP_ACC Access Control Policy

FDP_ACC.2 Complete Access Control

FDP_ACC.2.1 The TSF shall enforce the **access control policy** on **communication requests between the TOE_{OU} and other TOEs** and all operations among subjects and objects covered by the SFP.

FDP_ACC2.2 The TSF shall ensure that all operations between any subject in the TSC and any object within the TSC are covered by an access control SFP.

Dependencies:

FDP_ACF.1 Security Attribute Based Access Control

FDP_ACF Access Control Functions

FDP_ACF.1 Security Attribute Based Access Control

FDP_ACF.1.1 The TSF shall enforce the **access control policy** to objects based on **the TOE_{OU}'s credentials incorporated within it's assigned X.509 certificate, authentication of the TOE_{OU}'s cryptographically bound authentication data, and verification of the TOE_{OU}'s authorisation to interconnect as reported in the current TOE access control list.**

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

Connectivity between an OU site AU and a recipient are allowed provided the following conditions are met:

for transmissions from an OU site AU (transmission out of an OU site, high-side to low-side)

- **The transmitting OU site AU's IP address and password must be verified and on the transmitting TOE_{OU} site's access control list, and**
- **the transmitting TOE_{OU} and recipient TOE must mutually authenticate each other's cryptographically bound authentication data, or**

for transmissions to an OU site AU (transmissions into an OU site, low-side to high-side)

- **The destination OU site AU's IP address must be on the recipient TOE_{OU}'s site's access control list, and**
- **the transmitting TOE must be identified on the recipient TOE_{OU}'s access control list, and**

- **the recipient TOE$_{OU}$ and the originating TOE must mutually authenticate each other's cryptographically bound authentication data prior to the exchange of user data.**

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **valid key exchange**.

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the **None**.

Dependencies:

FDP_ACC.1 Subset Access Control

FMT_MSA.3 Static Attribute Initialisation

FDP_ETC Export to Outside the TSF Control

FDP_ETC.1 Export of User Data Without Security Attributes

FDP_ETC.1.1 The TSF shall enforce the **removing of security attributes upon receipt of data from another TOE** when exporting user data **to an OU site recipient Authorised User**, controlled under the SFP(s), outside of the TSC.

FDP_ETC.1.2 The TSF shall export the user data without the *transmitting TOE's* associated security attributes.

Dependencies:

[FDP_ACC.1 Subset access control, or

FDP_IFC.1 Subset information flow control]

FDP_ETC.2 Export of User Data With Security Attributes

FDP_ETC.2.1 The TSF shall enforce the **application of security attributes** when exporting user data **from the TOE$_{OU}$ destined to another TOE**, controlled under the SFP(s), outside of the TSC.

FDP_ETC.2.2 The TSF shall export the user data with the user data's associated security attributes.

FDP_ETC.2.3 The TSF shall ensure that the security attributes, when exported outside the TSC, are unambiguously associated with the exported user data.

FDP_ETC.2.4 The TSF shall enforce the following rules when user data is exported from the TSC: **the transmitting TOE$_{OU}$ must provide confidentiality, integrity protection, source authentication, and replay prevention**.

Dependencies:

[FDP_ACC.1 Subset access control, or

FDP_IFC.1 Subset information flow control]

FDP_ITC Import from Outside TSF Control

FDP_ITC.2 Import of User Data With Security Attributes

FDP_ITC.2.1 The TSF shall enforce the verification of certificate based data source authentication and integrity protection, public key exchanges, data decryption, and identity based access control lists when importing user data, controlled under the SFP(s), from outside of the TSC

FDP_ITC.2.2 The TSF shall use the security attributes associated with the imported user data.

FDP_ITC.2.3 The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received.

FDP_ITC.2.4 The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.

FDP_ITC.2.5 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: **None**.

Dependencies: [FDP_ACC.1 Subset access control, or

FDP_IFC.1 Subset information flow control]

[FTP_ITC.1 Inter-TSF trusted channel, or

FTP_TRP.1 Trusted path]

FPT_TDC.1 Inter-TSF basic TSF basic TSF data consistency

FDP_RIP Residual Information Protection

FDP_RIP.2 Full Residual Information Protection

FDP_RIP.2.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the *allocation of the resource to* all objects.

Class FIA: Identification and Authentication

FIA_AFL Authentication Failures

FIA_AFL.1 Authentication Failure Handling

FIA_AFL.1.1 The TSF shall detect when **a Security Administrator configured number between one (1) and five (5)** unsuccessful authentication attempts occur related to **cumulative authentication failures of:**

a. **a specific user's asserted IP address and verified, uniquely assigned authorised user passwords.**

b. **System Administrator's authenticated identity to the TOE administrative functions,**

c. **transmitting TOE's authenticated identity to receive TOE access control list.**

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall **lock the Unauthorised Agent (UA), or Authorised User (AU) out; discontinue processing attempts to authenticate the UA or AU; notify both System & Security Administrators for subsequent action.**

Dependencies:

FIA_UAU.1 Timing of authentication

FIA_ATD User Attribute Definition

FIA_ATD.1 User Attribute Definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: **IP address, X.509 certificate, passwords, TOE association, defined role {e.g. AU, Sec Admin, Sys Admin**}

FIA_SOS Specification of Secrets

FIA_SOS.1 Verification of Secrets

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet **an appropriate bit length in accordance with specified algorithm and key length, and not key that is all ones, all zeros, or repeating patterns.**

FIA_SOS.2 TSF Generation of Secrets

FIA_SOS.2.1 The TSF shall provide a mechanism to generate secrets that meet **an appropriate bit length in accordance with specified algorithm and key length, and not key that is all ones, all zeros, or repeating patterns.**

FIA_SOS.2.2 The TSF shall be able to enforce the use of TSF generated secrets for **unique TOE-to-TOE session keys.**

FIA_UAU User Authentication

FIA_UAU.2 User Authentication Before any Action

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of the user.

Dependencies:

FIA_UID.1 Timing of identification

FIA_UAU.3 Unforgeable Authentication

FIA_UAU.3.1 The TSF shall *prevent* use of authentication data that has been forged by any user of the TSF.

FIA_UAU.3.2 The TSF shall *prevent* use of authentication data that has been copied from any other user of the TSF.

FIA_UAU.5 Multiple Authentication Mechanisms

FIA_UAU.5.1 The TSF shall provide **AU IP address, hardware token and interface, and unique ID** to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the **IP address of their assigned host terminal and the associated TOE access control list, Remote User's X.509 certificate based authenticated identity and associated TOE access control list, unique ID established by an authenticated identity transaction, administrator's X.509 certificate based authenticated identity and established TOE administrator access control list.**

FIA_UAU.6 Re-authenticating

FIA_UAU.6.1 The TSF shall re-authenticate the user under the conditions **continuously within each protected datagram for TOE-to-TOE connections, with each datagram received from local AU's by comparing the attached IP address to the access control list**.

FIA_UAU.7 Protected authentication feedback

FIA_UAU.7.1 The TSF shall provide only **acknowledgement of data entry** to the user while the authentication is in progress.

Dependencies:

FIA_UAU.1 Timing of authentication

Application note: The authentication data that is provided by direct user entry shall not be displayed. In particular, if the user is required to enter a password at a keyboard for authentication, the password should not be displayed, but it would be desirable to display a positive acknowledgement of each keystroke.

FIA_UID User Identification

FIA_UID.2 User Identification Before Any Action

FIA_UID.2.1 The TSF shall require each user to identify itself before allowing any other TSF mediated actions on behalf of that user.

FIA_USB User-subject Binding

FIA_USB.1 User-subject Binding

FIA_USB.1.1 The TSF shall associate the appropriate user security attributes with subjects acting on behalf of that user.

Dependencies: FIA_ATD.1 User Attribute Definition

Class FMT: Security Management

FMT_MOF Management of Functions in TSF

FMT_MOF.1 Management of Security Functions Behaviour

FMT_MOF.1.1 The TSF shall restrict the ability to *determine the behaviour of, disable, enable, modify the behaviour of* the functions **user accounts, selecting auditable events, managing the audit trail, access control lists** to **System and Security Administrators**.

Dependencies:

FMT_SMR.1 Security Roles

FMT_MSA Management of Security Attributes

FMT_MSA.1 Management of Security Attributes

FMT_MSA.1.1 The TSF shall enforce the **access control security policy** to restrict the ability to *change, default, query, modify, delete*, ***create*** the security attributes **selecting auditable events, access control lists, managing audit trails, user accounts** to **System and Security Administrators**.

Dependencies:

[FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security Roles

FMT_MSA.2 Secure Security Attributes

FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for security attributes.

Dependencies:

ADV_SPM.1 Informal TOE security policy model

[FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control]

FMT_MSA.1 Management of security attributes

FMT_SMR.1 Security Roles

FMT_MSA.3 Static Attribute Initialisation

FMT_MSA.3.1 The TSF shall enforce **access control security policy, information flow control security policy** to provide *restrictive* default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the **Security Administrator** to specify alternative initial values to override the default values when an object or information is created.

Dependencies: FMT_MSA.1 Management of security attributes

FMT_SMR.1 Security Roles

FMT_MTD Management of TSF Data

FMT_MTD.1 Management of TSF Data

FMT_MTD.1.1 The TSF shall restrict the ability to *change-default, query, modify, delete, clear,* ***define*** the **selectable audit events, management of audit trails, user account privileges, AU access control lists and peer TOE access control lists** to **the Security Administrator**.

FMT_MTD.1.1 The TSF shall restrict the ability to *query, delete, clear,* ***add*****,** ***establish*** the **system back ups, register users, establish host addresses, system patches** to **the System Administrator**.

Dependencies:

FMT_SMR.1 Security Roles

FMT_MTD.2 Management of Limits on TSF Data

FMT_MTD.2.1 The TSF shall restrict the specification of the limits for **Accounts of users who no longer need access, user passwords more then 60 days old, keys that have expired, the temporary audit storage to be no larger than 5 Megs or older than 24 hours** to **the Security Administrator.**

FMT-MTD.2.2 The TSF shall take the following actions, if the TSF data are at, or exceed, the indicated limits: **Users accounts that no longer need access are deleted; passwords more then 60 days old – send a message to the user and lock the account until it is changed; X.509 certificates that have expired – obtain a new certificate; send a message to the System and Security Administrators to record the event and take appropriate action.**

Dependencies:

FMT_MTD.1 Management of TSF data

FMT_SMT.1 Security Roles

FMT_MTD.3 Secure TSF Data

FMT_MTD.3.1 The TSF shall ensure that only secure values are accepted for TSF data.

Dependencies:

ADV_SPM.1 Informal TOE security policy model

FMT_MTD.1 Management of TSF data

FMT_SMR Security Management Roles

FMT_SMR.2 Restrictions on Security Roles

FMT_SMR.2.1 The TSF shall maintain the roles **System Administrator, Security Administrator, and Authorised User.**

FMT_SMR.2.2 The TSF shall be able to associate users with roles.

FMT_SMR.2.3 The TSF shall ensure that the conditions **X.509 certificate extension designates System Administrators, Security Administrators, and Remote User roles, associated IP address designates local Authorised Users** are satisfied.

FMT_SMR.3 Assuming Roles

FMT_SMR.3.1 The TSF shall require an explicit request to assume the following roles: **System Administrator and Security Administrator.**

Dependencies:

FMT_SMR.1 Security Roles

Class FPR: Privacy

FPR_ANO Anonymity

FPR_ANO.1 Anonymity

FPR_ANO.1.1 The TSF shall ensure that **parties on public networks** are unable to determine the real user name bound to **datagrams.**

FPR_UNO Unobservability

FPR_UNO.4 Authorised User Observability.

FPR_UNO.4.1 The TSF shall provide **the System and Security Administrators** with the capability to observe the usage of **TOE resources and processes**.

Class FPT: Protection of TOE Security Functions

FPT_AMT Underlying Abstract Machine Test

FPT_AMT.1 Abstract Machine Test

FPT_AMT.1.1 The TSF shall run a suite of tests *during initial start-up, periodically during normal operation, and at the request of an Authorised Administrator* to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the TSF

FPT_FLS Fail Secure

FPT_FLS.1 Failure with Preservation of Secure State

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: **power failure, detection of an insecure operation, detection of an unknown state**.

Dependencies:

ADV_SPM.1 Informal TOE security policy model

FPT_ITI Integrity of Exported TSF Data

FPT_ITI.1 Inter-TSF Detection of Modification

FPT_ITI.1.1 The TSF shall provide the capability to detect modification of all TSF data during transmission between the TSF and a remote trusted IT product within the following metric: **the strength must be conformant to the strength offered by SHA-1 and DSA or RSA.**

.

FPT_ITI.1.2 The TSF shall provide the capability to verify the integrity of all TSF data transmitted between the TSF and a remote trusted IT product and perform **a retransmission and generate an audit record** if modifications are detected.

FPT_PHP TSF Physical Protection

FPT_PHP.1 Passive Detection of Physical Attack

FPT_PHP.1.1 The TSF shall provide unambiguous detection of physical tampering that might compromise the TSF.

FPT_PHP.1.2 The TSF shall provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred.

Dependencies:

FMT_MOF.1 Management of security function's behaviour

FPT_RCV Trusted Recovery

FPT_RCV.2 Automated Recovery

FPT_RCV.2.1 When automated recovery from a failure or service discontinuity is not possible, the TSF shall enter a maintenance mode where the ability to return the TOE to a secure state is provided.

FPT_RCV.2.2 For **power failures and loss of bit count integrity** the TSF shall ensure the return of the TOE to a secure state using automated procedures.

Dependencies:

FPT_TST.1 TSF testing

AGD_ADM.1 Administrator guidance

ADV_SPM.1 Informal TOE security model

FPT_RPL Replay Detection

FPT_RPL.1 Replay Detection

FPT_RPL.1.1 The TSF shall detect replay for the following entities: **TOE to TOE transmissions, .Authorised Administrator access.**

FPT_RPL.1.2 The TSF shall **ignore the attempted replay operation and generate an audit record** when replay is detected.

FPT_RVM Reference Mediation

FPT_RVM.1 Non-bypassability of the TSP

FPT_RVM.1.1 The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

FPT_SEP Domain Separation

FPT_SEP.1 TSF Domain Separation

FPT_SEP.1.1 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2 The TSF shall enforce separation between the security domains of subjects in the TSC.

FPT_STM Time Stamps

FPT_STM.1 Reliable Time Stamps

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps for its own use.

FPT_TDC Inter-TSF TSF Data Consistency

FPT_TCC.1 Inter-TSF Basic TSF Data Consistency

FPT_TDC.1.1 The TSF shall provide the capability to consistently interpret **audit records, security back up parameters, delivery notices, and key management data** when shared between the TSF and another trusted IT product.

FPT_TDC.1.2 The TSF shall use **developer specified protocols (in the Security Target) which conform with best commercial practice** when interpreting the TSF data from another trusted IT product.

FPT_TST TSF Self Test

FPT_TST.1 TSF Testing

FPT_TST.1.1 The TSF shall run a suite of self-tests *during initial start-up, periodically during normal operation, at the request of the System or Security Administrators* to demonstrate the correct operation of the TSF.

FPT_TST.1.2 The TSF shall provide **System and Security Administrators** with the capability to verify the integrity of TSF data.

FPT_TST.1.3 The TSF shall provide **System and Security Administrators** with the capability to verify the integrity of stored TSF executable code.

Dependencies:

FPT_AMT.1 Abstract machine testing

Class FRU: Resource Utilisation

FRU_FLT Fault Tolerance

FRU_FLT.1 Degraded Fault Tolerance

FRU_FLT.1.1 The TSF shall ensure that operation of **the following TOE mechanisms: file and configuration parameters, automatic back up, suspend processing, and default to a secure state** when the following failures occur: **loss of power to the TOE, detection of security relevant failures, detection of security policy violations, notification by the Misuse Detection system**.

Dependencies:

FPT_FLS.1 Failure with preservation of secure state

FRU_RSA Resource Allocation

FRU_RSA.1 Maximum Quotas

FRU_RSA.1.1 The TSF shall enforce maximum quotas of the following resources: **total throughput capacity of TOE** that an **individual user** can use **over a specified period of time**.

Class FTA: TOE Access

FTA_MCS Limitation on Multiple Concurrent Sessions

FTA_MCS.1 Basic Limitation on Multiple Concurrent Sessions

FTA_MCS.1.1 The TSF shall restrict the maximum number of concurrent sessions that belong to the same user.

FTA_MCS.1.2 The TSF shall enforce, by default, a limit of **an administrator selectable fixed number (between three and 99) of concurrent** sessions per user.

Application Note: The allowable range of concurrent sessions will be established by policy and set by the System or Security Administrator. The TOE must allow for selection within a range of three to 99.

Dependencies:

FIA_UID.1 Timing of identification

FTA_SSL Session Locking

FTA_SSL.3 TSF-Initiated Termination

FTA_SSL.3.1 The TSF shall terminate an interactive session after **an administrator selectable TOE parameter which establishes the termination inactivity period between the range of five to 60 minutes.**

Application Note: The interactive session, which is terminated, is between the transmitting TOE_{OU} and the destination TOE. The results of user inactivity will require the transmitting TOE_{OU} to establish a new session with the recipient TOE.

FTA_TSE TOE Session Establishment

FTA_TSE.1 TOE Session Establishment

FTA_TSE.1.1 The TSF shall be able to deny session establishment based on **invalid user IP address, password or invalid System or Security Administrator authentication identities.**

Class FTP: Trusted Path/Channels

FTP_ITC Inter-TSF Trusted Channel

FTP_ITC.1 Inter-TSF Trusted Channel

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit *the remote trusted IT product* to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for **transfer of user, audit and administrative data**.

5.2 TOE$_{RU}$ Security Functional Requirements

The functional security requirements for the TOE$_{RU}$ consist of the following components derived from Part 2 of the CC and are summarised in Table 3.

Table 3 TOE$_{RU}$ Functional Security Requirements Summary

Requirement Class	Requirement Family	Requirement Component
FAU – Security Audit	ARP – Security Alarm	.1 Security Alarm
	GEN – Security Audit Generation	.1 Audit Data Generation
		.2 User Identity Association
	SAR – Security Audit Review	.1 Audit Review
	SEL – Selective Audit	.1 Selective Audit
FCO – Communication	None	None
FCS – Cryptographic Support	CKM – Cryptographic Key Management	.1 Crypto Key Generation
		.2 Crypto Key Distribution
		.4 Crypto Key Destruction
	COP – Cryptographic Operation	.1 Cryptographic Operation
FDP – User Data Protection	ACC- Access Control Policy	.2 Complete Access Control
	ACF – Access Control Functions	.1 Security Attribute Based Access Control

(continued) FDP – User Data Protection	ETC – Export of User Data w/o Security Attributes	.1 Export of User Data w/o Security Attributes
		.2 Export of User Data with Security Attributes
	ITC – Import of User Data with Security Attributes	.2 Import of User Data with Security Attributes
	RIP – Residual Information Protection	.2 Full Residual Info Protection
FIA – Identification & Authentication	AFL – Authentication Failures	.1 Authentication Failure Handling
	ATD – User Attribute Definition	.1 User Attribute Definition
	SOS – Specification of Secrets	.1 Verification of Secrets
		.2 TSF Generation of Secrets
	UAU – User Authentication	.2 User Authentication Before any Action
		.3 Unforgeable Authentication
		.5 Multiple Authentication Mechanisms
		.6 Re-authenticating
	UID – User Identification	.2 User ID Before any Action
	USB – User-subject Binding	.1 User-subject Binding

FMT – Security Management	MOF – Management of Functions in TSF	.1 Management of Security Functions Behaviour
	MSA – Management of Security Attributes	.1 Management of Security Attributes
		.2 Secure Security Attributes
		.3 Static Attribute Initialisation
	MTD – Management of TSF Data	.1 Management of TSF Data
		.2 Management of Limits on TSF Data
		.3 Secure TSF Data
	SMR – Security Management Roles	.2 Restrictions on Security Roles
		.3 Assuming Roles
FPR – Privacy	ANO - Anonymity	.1 Anonymity
	UNO - Observability	.4 Authorised User Observability
FPT – Protection of TOE Security Functions	AMT – Underlying Abstract Machine Test	.1 Abstract Machine Test
	FLS – Fail Safe	.1 Failure with Preservation of Secure Path
	ITI – Integrity of Exported TSF Data	.1 Inter-TSF Detection of Modification
	PHP – TSF Physical Protection	.1 Passive Detection of Physical Attack
	RCV – Trusted Recovery	.2 Automatic Recovery
	RPL – Replay Detection	.1 Replay Detection
	RVM – Reference Mediation	.1 Non-bypassability
	SEP – Domain Separation	.1 TSF Domain Separation

FPT – (cont.) Protection of TOE Security Functions	STM – Time Stamps	.1 Reliable Time Stamps
	TDC – Inter-TSF TSF Data Consistency	.1 Inter-TSF Basic TSF Data Consistency
	TST – TSF Self Test	.1 TSF Testing
FRU – Resource Utilisation	FLT – Fault Tolerance	.1 Degraded Fault Tolerance
FTA – TOE Access	LSA – Limitation on Scope of Selectable Attributes	.1 Limitation on Scope of Selectable Attributes
	MCS – Limitation on Multiple Concurrent Sessions	.1 Basic Limitation on Multiple Concurrent Sessions
	SSL – Session Locking	.3 TSF-Initiated Termination
	TSE – TOE Session Establishment	.1 TOE Session Establishment
FTP – Trusted Path/Channels	ITC – Inter-TSF Trusted Channel	.1 Inter-TSF Trusted Channel

Class FAU: Security Audit

FAU_ARP Security Audit Automatic Response

FAU_ARP.1 Security Alarms

FAU_ARP.1.1 The TSF shall take **action to: detect audit events, alert Remote User and System and Security Administrators, generate and transmit audit records to an associated Misuse Detection System** upon detection of a potential security violation.

Dependencies:

FAU_SAA.1 Potential Violation Analysis

FAU_GEN Security Audit Data Generation

FAU_GEN.1 Audit Data Generation

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a. Start-up and shutdown of the audit functions;

b. All auditable events for the *basic* level of audit; and

c. The specifically detailed audit events listed in Appendix B.

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a. Date and time of the event, type of event, and subject identity, and the outcome (success or failure) of the event; and

b. For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, **none.**

Dependencies:

FPT_STM.1 Reliable Time Stamps

FAU_GEN.2 User Identity Association

FAU_GEN.2.1 The TSF shall be able to associate each auditable event with the identity of the user that caused the event.

Dependencies:

FAU_GEN.1 Audit Data Generation

FIA_UID.1 Timing of Identification

FAU_SAR Security Audit Review

FAU_SAR.1 Audit Review

FAU_SAR.1.1 The TSF shall provide **the Remote User and the Misuse Detection system** with the capability to read **all audit data** from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information**.**

Dependencies:

FAU_GEN.1 Audit Data Generation

FAU_SEL Security Audit Event Selection

FAU_SEL.1 Selective Audit

FAU_SEL.1.1 The TSF shall be able to include or exclude auditable events from the set of audited events based on the following attributes:

a. ***specific file*** *identity, user identity,* ***specific process*** *identity, host identity, event type*

b. **time of day, date**

Dependencies:

FAU_GEN.1 Audit Data Generation

FMT_MTD.1 Management of TSF Data

Application Note: There is no intent to require the TOE to store audit records. What is required is the TOE must cryptographically protect the audit record before sending it to the Misuse Detection system for storage and analysis. Please note that FTP_ITC.1.3, Trusted Channels, supports this requirement.

Class FCS: Cryptographic Support

FCS_CKM Cryptographic Key Management

FCS_CKM.1 Cryptographic Key Generation

FCS_CKM.1.1 The TSF shall generate cryptographic key in accordance with a specified cryptographic key generation algorithm **pseudo-random number generation, Diffie Hellman exponents,** and specified cryptographic key sizes **equivalent to or great than 112 bits of protection** that meets the following: **FIPS 140-2, Level 2**.

Dependencies:

[FCS_CKM.2 Cryptographic Key Distribution, or FCS_COP.1 Cryptographic Operation]

FCS_CKM.4 Cryptographic Destruction

FMT_MSA.2 Secure security attributes

FCS_CKM.2 Cryptographic Key Distribution

FCS_CKM.2.1 The TSF shall distribute cryptographic key in accordance with a specified cryptographic key distribution method **DoD medium assurance PKI for public key distribution using Class 4 X.509, version 3 certificates with hardware tokens for protection of private key used by Remote Users** that meets the following: **DoD PKI Roadmap and ANSI X9.6**.

Dependencies:

[FDP_ITC.1 Import of User Data Without Security Attributes, or

FCS_CKM.1 Cryptographic Key Generation]

FCS_CKM4 Cryptographic Key Destruction

FMT_MSA.2 Secure Security Attributes

FCS_CKM.4 Cryptographic Key Destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic key in accordance with a specified cryptographic key destruction method **zeroization of all plain text cryptographic keys and other critical security parameters within the device** that meets the following: **FIPS 140-2, Level 2**.

Dependencies:

[FDP_ITC.1 Import of User Data Without Security Attributes, or

FCS_CKM.1 Cryptographic Key Generation]

FMT_MSA.2 Secure security attributes

FCS_COP Cryptographic Operation

FCS_COP.1 Cryptographic Operation

FCS_COP.1.1 The TSF shall perform **data encryption services** in accordance with a specified cryptographic algorithm and cryptographic key **168 bits (equivalent to at least 112 bits of security protection) for 3DES** that meet the following: **Draft NIST FIPS Pub 46-3 for 3DES, Internet Engineering Task Force Request for Comment (RFC) 2401, “Security Architecture for the Internet Protocol,” and RFC 2406, “IP Encapsulating Security Payload, Tunnel Mode**”.

Dependencies:

[FDP_ITC.1 Import of User Data Without Security Attributes, or

FCS_CKM.1 Cryptographic Key Generation]

FCS_CKM.4 Cryptographic key destruction

FMT_MSA.2 Secure security attributes

Application Note: Future migration to incorporate the Advanced Encryption Standard (AES) is anticipated and will be approved when standards are established.

FCS_COP.1.1 The TSF shall perform **data source authentication and integrity protection** in accordance with a specified cryptographic algorithm **HMAC with SHA-1** and cryptographic key sizes **160 bits** that meet the following: **RFC 2104, “Keyed-Hashing for Message Authentication, dated February, 1997, and RFC 2404, “Use of HMAC-SHA-1-96 within ESP and AH”**.

Dependencies:

[FDP_ITC.1 Import of User Data Without Security Attributes, or

FCS_CKM.1 Cryptographic Key Generation]

FCS_CKM.4 Cryptographic key destruction

FMT_MSA.2 Secure security attributes

Application Note: The Digital Signature Algorithm (DSA) is also acceptable and future migration to incorporate NIST approved Elliptic Curve DSA will be acceptable when standards are established.

FCS_COP.1.1 The TSF shall perform **hashing** in accordance with a specified cryptographic algorithm **Security Hash Algorithm 1 (SHA-1)** and cryptographic key sizes **160 bits** that meet the following: **FIPS 180-1**.

Dependencies:

[FDP_ITC.1 Import of User Data Without Security Attributes, or

FCS_CKM.1 Cryptographic Key Generation]

FCS_CKM.4 Cryptographic Key Destruction

FMT_MSA.2 Secure Security Attributes

FCS_COP.1.1 The TSF shall perform **key exchange** in accordance with a specified cryptographic algorithm **Diffie-Helman Algorithm** and cryptographic key sizes **of at least 1024 bits (or NIST Elliptic Curves that provide equivalent or better strength)** that meet the following: **Internet Engineering Task Force, Request for Comment (RFC) 2401, “Security Architecture for the Internet Protocol”; and RFC 2409, “The Internet Key Exchange (IKE)” using ESP, Tunnel Mode, Main Mode, Public Key Signatures.**

Dependencies:

[FDP_ITC.1 Import of user data without security attributes or

FCS_CKM.1 Cryptographic Key Generation]

FCS_CKM.4 Cryptographic Key Destruction

FMT_MSA.2 Secure Security Attributes

Class FDP: User Data Protection

FDP_ACC Access Control Policy

FDP_ACC.2 Complete Access Control

FDP_ACC.2.1 The TSF shall enforce the **access control policy** on **communication requests between the TOE_{RU} and other TOEs** and all operations among subjects and objects covered by the SFP.

FDP_ACC2.2 The TSF shall ensure that all operations between any subject in the TSC and any object within the TSC are covered by an access control SFP.

Dependencies:

FDP_ACF.1 Security Attribute Based Access Control

FDP_ACF Access Control Functions

FDP_ACF.1 Security Attribute Based Access Control

FDP_ACF.1.1 The TSF shall enforce the **access control policy** to objects based on **the TOE_{RU}'s credentials incorporated within it's assigned X.509 certificate, authentication of the TOE_{RU}'s cryptographically bound authentication data, and verification of the TOE_{RU}'s authorisation to interconnect as reported in the current TOE access control list.**

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

Connectivity between a RU site TOE_{RU} and the RU site's associated OU site TOE_{OU} is allowed provided the following conditions are met:

- **all transmissions must be between the TOE_{RU} and the TOE_{RU}'s associated home OU site as established by the current TOE_{RU} access control list, and**

- **the TOE_{RU} and the associated home OU site TOE_{OU} must mutually authenticate each other's cryptographically bound authentication data.**

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **valid key exchange**.

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the **None**.

Dependencies:

FDP_ACC.1 Subset Access Control

FMT_MSA.3 Static Attribute Initialisation

FDP_ETC Export to Outside the TSF Control

FDP_ETC.1 Export of User Data Without Security Attributes

FDP_ETC.1.1 The TSF shall enforce the **removing of security attributes upon receipt of data from its associated TOE$_{OU}$** when exporting user data **to the authorised remote user**, controlled under the SFP(s), outside of the TSC.

FDP_ETC.1.2 The TSF shall export the user data without the user data's associated security attributes.

Dependencies:

[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]

FDP_ETC.2 Export of User Data With Security Attributes

FDP_ETC.2.1 The TSF shall enforce the **application of security attributes** when exporting user data **from the TOE$_{RU}$ to another TOE**, controlled under the SFP(s), outside of the TSC.

FDP_ETC.2.2 The TSF shall export the user data with the user data's associated security attributes.

FDP_ETC.2.3 The TSF shall ensure that the security attributes, when exported outside the TSC, are unambiguously associated with the exported user data.

FDP_ETC.2.4 The TSF shall enforce the following rules when user data is exported from the TSC: **the transmitting TOE$_{RU}$ must provide confidentiality, integrity protection, source authentication, and replay prevention**.

Dependencies:

[FDP_ACC.1 Subset access control, or

FDP_IFC.1 Subset information flow control]

FDP_ITC Import from Outside TSF Control

FDP_ITC.2 Import of User Data With Security Attributes

FDP_ITC.2.1 **The** TSF shall enforce the **verification of certificate based data source authentication and integrity protection, public key exchanges, data decryption, and identity based access control lists** when importing user data, controlled under the SFP(s), from outside of the TSC.

FDP_ITC.2.2 The TSF shall use the security attributes associated with the imported user data.

FDP_ITC.2.3 The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and the user data received.

FDP_ITC.2.4 The TSF shall ensure that interpretation of the security attributes of the imported user data is as intended by the source of the user data.

FDP_ITC.2.5 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: **None**.

Dependencies:

[FDP_ACC.1 Subset access control, or

FDP_IFC.1 Subset information flow control]

[FTP_ITC.1 Inter-TSF trusted channel, or

FTP_TRP.1 Trusted path]

FPT_TDC.1 Inter-TSF basic TSF basic TSF data consistency

FDP_RIP Residual Information Protection

FDP_RIP.2 Full Residual Information Protection

FDP_RIP.2.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the *allocation of the resource to* all objects.

Class FIA: Identification and Authentication

FIA_AFL Authentication Failures

FIA_AFL.1 Authentication Failure Handling

FIA_AFL.1.1 The TSF shall detect when a Security Administrator configured number between one (1) and five (5) unsuccessful authentication attempts occur related to cumulative authentication failures of:

a. **a specific user's authentication identity and provided password verified by $\mathbf{TOE_{RU}}$ access control list,**

b. **System or Security Administrator's authentication identity and password to $\mathbf{TOE_{RU}}$ administrative functions,**

c. **transmitting $\mathbf{TOE_{RU}}$'s authentication identity to recipient $\mathbf{TOE_{OU}}$'s access control list.**

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall lock the Unauthorised Agent (UA), or Remote User (RU) out; discontinue processing attempts to authenticate the UA or RU; notify both System & Security Administrators for subsequent action.

Dependencies:

FIA_UAU.1 Timing of authentication

FIA_ATD User Attribute Definition

FIA_ATD.1 User Attribute Definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: **X.509 certificate, private authentication data and private key exchange keys, passwords, TOE association, defined role {e.g. RU, Sec Admin, Sys Admin**}.

FIA_SOS Specification of Secrets

FIA_SOS.1 Verification of Secrets

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet **an appropriate bit length in accordance with specified algorithm and key length, and not key that is all ones, all zeros, or repeating patterns.**

FIA_SOS.2 TSF Generation of Secrets

FIA_SOS.2.1 The TSF shall provide a mechanism to generate secrets that meet an appropriate bit length in accordance with specified algorithm and key length, and not key that is all ones, all zeros, or repeating patterns.

FIA_SOS.2.2 The TSF shall be able to enforce the use of TSF generated secrets for **unique TOE$_{RU}$-to-TOE$_{OU}$ session keys.**

FIA_UAU User Authentication

FIA_UAU.2 User Authentication Before any Action

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of the user.

Dependencies:

FIA_UID.1 Timing of identification

FIA_UAU.3 Unforgeable Authentication

FIA_UAU.3.1 The TSF shall *prevent* use of authentication data that has been forged by any user of the TSF.

FIA_UAU.3.2 The TSF shall prevent use of authentication data that has been copied from any other user of the TSF.

FIA_UAU.5 Multiple Authentication Mechanisms

FIA_UAU.5.1 The TSF shall provide password, hardware token and interface, and unique ID to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the password, user ID, Remote User's X.509 certificate based authentication identity and associated TOE$_{RU}$ access control list, and administrator's X.509 certificate based authentication identity and established TOE administrator access control list.

FIA_UAU.6 Re-authenticating

FIA_UAU.6.1 The TSF shall re-authenticate the user under the conditions continuously within each protected datagram for TOE-to-TOE connections.

FIA_UAU.7 Protected authentication feedback

FIA_UAU.7.1 The TSF shall provide only acknowledgement of data entry to the user while the authentication is in progress.

Dependencies:

FIA_UAU.1 Timing of authentication

Application note: The authentication data that is provided by direct user entry shall not be displayed. In particular, if the user is required to enter a password at a keyboard for authentication, the password should not be displayed, but it would be desirable to display a positive acknowledgement of each keystroke.

FIA_UID User Identification

FIA_UID.2 User Identification Before Any Action

FIA_UID.2.1 The TSF shall require each user to identify itself before allowing any other TSF mediated actions on behalf of that user.

FIA_USB User-subject Binding

FIA_USB.1 User-subject Binding

FIA_USB.1.1 The TSF shall associate the appropriate user security attributes with subjects acting on behalf of that user.

Dependencies:

FIA_ATD.1 User Attribute Definition

Class FMT: Security Management

FMT_MOF Management of Functions in TSF

FMT_MOF.1 Management of Security Functions Behaviour

FMT_MOF.1.1 The TSF shall restrict the ability to *determine the behaviour of, disable, enable, modify the behaviour of* the functions **user accounts, selecting auditable events, managing the audit trail, access control lists** to **System and Security Administrators**.

Dependencies:

FMT_SMR.1 Security Roles

FMT_MSA Management of Security Attributes

FMT_MSA.1 Management of Security Attributes

FMT_MSA.1.1 The TSF shall enforce the **access control security policy** to restrict the ability to *change, default, query, modify, delete*, ***create*** the security attributes **selecting auditable events, access control lists, managing audit trails, user accounts** to **System and Security Administrators**.

Dependencies:

[FDP_ACC.1 Subset access control or

FDP_IFC.1 Subset information flow control]

FMT_SMR.1 Security Roles

FMT_MSA.2 Secure Security Attributes

FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for security attributes.

Dependencies:

ADV_SPM.1 Informal TOE security policy model

[FDP_ACC.1 Subset access control or

FDP_IFC.1 Subset information flow control]

FMT_MSA.1 Management of security attributes

FMT_SMR.1 Security Roles

FMT_MSA.3 Static Attribute Initialisation

FMT_MSA.3.1 The TSF shall enforce **access control security policy, information flow control security policy** to provide *restrictive* default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the **Security Administrator** to specify alternative initial values to override the default values when an object or information is created.

Dependencies:

FMT_MSA.1 Management of security attributes

FMT_SMR.1 Security Roles

FMT_MTD Management of TSF Data

FMT_MTD.1 Management of TSF Data

FMT_MTD.1.1 The TSF shall restrict the ability to *change-default, query, modify, delete, clear,* ***define*** the **selectable audit events, management of audit trails, user account privileges, RU access control lists and peer TOE$_{OU}$ access control list** to **the Security Administrator or their designee**.

FMT_MTD.1.1 The TSF shall restrict the ability to *query, delete, clear,* ***add*****,** ***establish*** the **system back ups, register users, establish host addresses, system patches** to **the System Administrator or their designee**.

Dependencies:

FMT_SMR.1 Security Roles

FMT_MTD.2 Management of Limits on TSF Data

FMT_MTD.2.1 The TSF shall restrict the specification of the limits for **Accounts of users who no longer need access, user passwords more then 60 days old, keys that have expired, the temporary audit storage to be no larger than 5 Megs or older than 24 hours** to **the Security Administrator**.

FMT-MTD.2.2 The TSF shall take the following actions, if the TSF data are at, or exceed, the indicated limits: **Users accounts that no longer need access are deleted; passwords more then 60 days old – send a message to the user and lock the account until it is changed; X.509 certificates that have expired – obtain a new certificate; send a message to the System and Security Administrators to record the event and take appropriate action.**

Dependencies:

FMT_MTD.1 Management of TSF data

FMT_SMT.1 Security Roles

FMT_MTD.3 Secure TSF Data

FMT_MTD.3.1 The TSF shall ensure that only secure values are accepted for TSF data.

Dependencies:

ADV_SPM.1 Informal TOE security policy model

FMT_MTD.1 Management of TSF data

FMT_SMR Security Management Roles

FMT_SMR.2 Restrictions on Security Roles

FMT_SMR.2.1 The TSF shall maintain the roles **System Administrator, Security Administrator and Authorised User**.

FMT_SMR.2.2 The TSF shall be able to associate users with roles.

FMT_SMR.2.3 The TSF shall ensure that the conditions **X.509 certificate extension designates System Administrators, Security Administrators, and Remote User roles, associated IP address designates Remote Users** are satisfied.

FMT_SMR.3 Assuming Roles

FMT_SMR.3.1 The TSF shall require an explicit request to assume the following roles: **System Administrator and Security Administrator**.

Dependencies:

FMT_SMR.1 Security Roles

Class FPR: Privacy

FPR_ANO Anonymity

FPR_ANO.1 Anonymity

FPR_ANO.1.1 The TSF shall ensure that **parties on public networks** are unable to determine the real user name bound to **datagrams**.

FPR_UNO Unobservability

FPR_UNO.4 Authorised User Observability

FPR_UNO.4.1 The TSF shall provide **the System and Security Administrators** with the capability to observe the usage of **TOE$_{RU}$ resources and processes**.

Class FPT: Protection of TOE Security Functions

FPT_AMT Underlying Abstract Machine Test

FPT_AMT.1 Abstract Machine Test

FPT_AMT.1.1 The TSF shall run a suite of tests *during initial start-up, periodically during normal operation, and at the request of an Authorised Administrator* to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the TSF.

FPT_FLS Fail Secure

FPT_FLS.1 Failure with Preservation of Secure State

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: **power failure, detection of an insecure operation, detection of an unknown state**.

Dependencies:

ADV_SPM.1 Informal TOE security policy model

FPT_ITI Integrity of Exported TSF Data

FPT_ITI.1 Inter-TSF Detection of Modification

FPT_ITI.1.1 The TSF shall provide the capability to detect modification of all TSF data during transmission between the TSF and a remote trusted IT product within the following metric: **the strength must be conformant to the strength offered by SHA-1 and DSA or RSA**.

FPT_ITI.1.2 The TSF shall provide the capability to verify the integrity of all TSF data transmitted between the TSF and a remote trusted IT product and perform **a retransmission and generate an audit record** if modifications are detected.

FPT_PHP TSF Physical Protection

FPT_PHP.1 Passive Detection of Physical Attack

FPT_PHP.1.1 The TSF shall provide unambiguous detection of physical tampering that might compromise the TSF.

FPT_PHP.1.2 The TSF shall provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred.

Dependencies:

FMT_MOF.1 Management of security function's behaviour

FPT_RCV Trusted Recovery

FPT_RCV.2 Automated Recovery

FPT_RCV.2.1 When automated recovery from a failure or service discontinuity is not possible, the TSF shall enter a maintenance mode where the ability to return the TOE to a secure state is provided.

FPT_RCV.2.2 For **power failures and loss of bit count integrity** the TSF shall ensure the return of the TOE to a secure state using automated procedures.

Dependencies:

FPT_TST.1 TSF testing

AGD_ADM.1 Administrator guidance

ADV_SPM.1 Informal TOE security model

FPT_RPL Replay Detection

FPT_RPL.1 Replay Detection

FPT_RPL.1.1 The TSF shall detect replay for the following entities: TOE to TOE transmissions, Authorised Administrator access.

FPT_RPL.1.2 The TSF shall ignore the attempted replay operation and generate an audit record when replay is detected.

FPT_RVM Reference Mediation

FPT_RVM.1 Non-bypassability of the TSP

FPT_RVM.1.1 The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

FPT_SEP Domain Separation

FPT_SEP.1 TSF Domain Separation

FPT_SEP.1.1 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2 The TSF shall enforce separation between the security domains of subjects in the TSC.

FPT_STM Time Stamps

FPT_STM.1 Reliable Time Stamps

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps for its own use.

FPT_TDC Inter-TSF TSF Data Consistency

FPT_TCC.1 Inter-TSF Basic TSF Data Consistency

FPT_TDC.1.1 The TSF shall provide the capability to consistently interpret **audit records, security back up parameters, delivery notices, and key management data** when shared between the TSF and another trusted IT product.

FPT_TDC.1.2 The TSF shall use developer specified protocols (in the Security Target) which conform with best commercial practice when interpreting the TSF data from another trusted IT product.

FPT_TST TSF Self Test

FPT_TST.1 TSF Testing

FPT_TST.1.1 The TSF shall run a suite of self-tests *during initial start-up, periodically during normal operation, at the request of the System or Security Administrators* to demonstrate the correct operation of the TSF.

FPT_TST.1.2 The TSF shall provide **System and Security Administrators** with the capability to verify the integrity of TSF data.

FPT_TST.1.3 The TSF shall provide **System and Security Administrators** with the capability to verify the integrity of stored TSF executable code.

Dependencies:

FPT_AMT.1 Abstract machine testing

Class FRU: Resource Utilisation

FRU_FLT Fault Tolerance

FRU_FLT.1 Degraded Fault Tolerance

FRU_FLT.1.1 The TSF shall ensure the operation of **the following TOE$_{RU}$ mechanisms: file and configuration parameters, automatic back up, suspend processing, and default to a secure state** when the following failures occur: **detection of security relevant failures, detection of security policy violations, notification by the Misuse Detection system**.

Dependencies:

FPT_FLS.1 Failure with preservation of secure state

Class FTA: TOE Access

FTA_MCS Limitation on Multiple Concurrent Sessions

FTA_MCS.1 Basic Limitation on Multiple Concurrent Sessions

FTA_MCS.1.1 The TSF shall restrict the maximum number of concurrent sessions that belong to the same user.

FTA_MCS.1.2 The TSF shall enforce, by default, a limit of an Administrator selectable **fixed number (between one (1) and 10) of** sessions per user.

Dependencies:

FIA_UID.1 Timing of identification

Application Note: The range of one (1) to 10 was selected because the remote environment is less secure than the OU environment. Hence, restrictions are appropriate.

FTA_SSL Session Locking

FTA_SSL.3 TSF-Initiated Termination

FTA_SSL.3.1 The TSF shall terminate an interactive session after **an administrator selectable TOE_{RU} parameter which establishes the termination of inactivity period between the range of five (5) to 60 minutes.**

Application Note: The interactive session, which is terminated, is between the transmitting TOE_{RU} and the destination TOE_{OU}. The results of user inactivity will require the transmitting TOE_{RU} to establish a new session with the recipient TOE.

FTA_TSE TOE Session Establishment

FTA_TSE.1 TOE Session Establishment

FTA_TSE.1.1 The TSF shall be able to deny session establishment based on **invalid remote user's password or lack of hardware token.**

Class FTP: Trusted Path/Channels

FTP_ITC Inter-TSF Trusted Channel

FTP_ITC.1 Inter-TSF Trusted Channel

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and a remote trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2 The TSF shall permit the remote trusted IT product to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for transfer of user, audit and administrative data.

5.3 TOE Security Assurance Requirements

This PP specifies assurance requirements for the system as a whole. It does not define an assurance level for each independent component. The security assurance requirements were derived from Part 3, Version 2, of the CC. The overall assurance level for the system is EAL 3 with the addition of ADV_SPM.1, Informal TOE Security Policy Model. The details of assurance requirements are listed only once; however, Application Notes for each independent partition are listed separately. EAL3 plus our recommend additional requirement is summarised in Table 3.

Table 4 TOE Assurance Requirements

Assurance Class	Assurance Components
Configuration Management (CM)	ACM_CAP.3 Authorisation Controls ACM_SCP.1 TOE CM Coverage
Delivery and operation	ADO_DEL.1 Delivery procedures ADO_IGS.1 Installation, generation and start-up procedures
Development	ADV_FSP.1 Informal functional specification ADV_HLD.2 Security enforcing high-level design ADV_RCR.1 Informal correspondence demonstration ADV_SPM.1 Informal TOE Security Policy Model
Guidance documents	AGD_ADM.1 Administrator guidance AGD_USR.1 User guidance
Life cycle support	ALC_DVS.1 Identification of security measures
Tests	ATE_COV.2 Analysis of coverage ATE_DPT.1 Testing: high-level design ATE_FUN.1 Functional testing ATE_IND.2 Independent testing – sample
Vulnerability assessment	AVA_MSU.1 Examination of guidance AVA_SOF.1 Strength of TOE security function evaluation AVA_VLA.1 Developer vulnerability analysis

ACM_CAP CM Capabilities

ACM_CAP.3 Authorisation controls

ACM_CAP.3.1D The developer shall provide a reference for the TOE.

ACM_CAP.3.2D The developer shall use a CM system

ACM_CAP.3.3D The developer shall provide CM documentation.

ACM_CAP.3.1C The reference for the TOE shall be unique to each version of the TOE.

ACM_CAP.3.2C The TOE shall be labelled with its reference.

ACM_CAP.3.3C The CM documentation shall include a configuration list and a CM plan.

ACM_CAP.3.4C The configuration list shall describe the configuration items that comprise the TOE.

ACM_CAP.3.5C The CM documentation shall describe the method used to uniquely identify the configuration items.

ACM_CAP.3.6C The CM system shall uniquely identify all configuration items.

ACM_CAP.3.7C The CM plan shall describe how the CM system is used.

ACM_CAP.3.8C The evidence shall demonstrate that the CM system is operating in accordance with the CM plan.

ACM_CAP.3.9C The CM documentation shall provide evidence that all configuration items have been and are being effectively maintained under the CM system.

ACM_CAP.3.10C The CM system shall provide measures such that only authorised changes are made to the configuration items.

ACM_CAP.3.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

Dependencies:

ACM_SCP.1 TOE CM Coverage

ALC_DVS.1 Identification of Security Measures

ACM_SCP CM Scope

ACM_SCP.1 TOE CM Coverage

ACM_SCP.1.1C The CM documentation shall show that the CM system, as a minimum, tracks the following items: the TOE implementation representation, design documentation, test documentation, user documentation, administrator documentation, and CM documentation.

ACM_SCP.1.2C The CM documentation shall describe how configuration items are tracked by the CM system.

ACM_SCP.1.1D The developer shall provide CM documentation.

ACM_SCP.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

Dependencies:

ACM_CAP.3 Authorisation Controls

ADO_DEL Delivery and Operation

ADO_DEL.1 Delivery procedures

ADO_DEL.1.1D The developer shall document procedures for delivery of the TOE or parts of it to the user.

ADO_DEL.1.2D The developer shall use the delivery procedures.

ADO_DEL.1.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user's site.

ADO_DEL.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADO_IGS Installation, Generation and Start-up

ADO_IGS.1 Installation, generation, and start-up procedures

ADO_IGS.1.1D The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.

ADO_IGS.1.1C The documentation shall describe the steps necessary for secure installation, generation, and start-up of the TOE.

ADO_IGS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADO_IGS.1.2E The evaluator shall determine that the installation, generation, and start-up procedures result in a secure configuration.

Dependencies:

AGD_ADM.1 Administrator Guidance

ADV_FSP Functional Specification

ADV_FSP.1 Informal functional specification

ADV_FSP.1.1D The developer shall provide a functional specification.

ADV_FSP.1.1C The functional specification shall describe the TSF and its external interfaces using an informal style.

ADV_FSP.1.2C The functional specification shall be internally consistent.

ADV_FSP.1.3C The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing details of effects, exceptions, and error messages, as appropriate.

ADV_FSP.1.4C The functional specification shall completely represent the TSF.

ADV_FSP.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.1.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security functional requirements.

Dependencies:

ADV_RCR.1 Informal Correspondence Demonstration

ADV_HLD High Level Design

ADV_HLD.2 Security enforcing high-level design

ADV_HLD.2.1D The developer shall provide the high-level design of the TSF.

ADV_HLD.2.1C The presentation of the high-level design shall be informal.

ADV_HLD.2.2C The high-level design shall be internally consistent.

ADV_HLD.2.3C The high-level design shall describe the structure of the TSF in terms of subsystems.

ADV_HLD.2.4C The high-level design shall describe the security functionality provided by each subsystem of the TSF.

ADV_HLD.2.5C The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software.

ADV_HLD.2.6C The high-level design shall identify all interfaces to the subsystems of the TSF.

ADV_HLD.2.7C The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible.

ADV_HLD.2.8C The high-level design shall describe the purpose and method of use of all interfaces to the subsystems of the TSF, providing details of effects, exceptions and error messages, as appropriate.

ADV_HLD.2.9C The high-level design shall describe the separation of the TOE into TSP-enforcing and other subsystems.

ADV_HLD.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_HLD.2.2E The evaluator shall determine that the high-level design is an accurate and complete instantiation of the TOE security functional requirements.

Dependencies:

ADV_FSP.1 Informal Functional Specification

ADV_RCR.1 Informal Correspondence Demonstration

ADV_RCR Representation Correspondence

ADV_RCR.1 Informal correspondence demonstration

ADV_RCR.1.1D The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.

ADV_RCR.1.1C For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.

ADV_RCR.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_SPM Security Policy Modelling

ADV_SPM.1 Informal TOE Security Policy Model

ADV_SPM.1.1D The developer shall provide a TSP model.

ADV_SPM.1.2D The developer shall demonstrate correspondence between the functional specification and the TSP model.

ADV_SPM.1.1C The TSP model shall be informal.

ADV_SPM.1.2C The TSP model shall describe the rules and characteristics of all policies of the TSP that can be modelled.

ADV_SPM.1.3C The TSP model shall include a rationale that demonstrates that it is consistent and complete with respect to all policies of the TSP that can be modelled.

ADV_SPM.1.4C The demonstration of correspondence between the TSP model and the functional specification shall show that all of the security functions in the functional specification are consistent and complete with respect to the TSP model.

ADV_SPM.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

Dependencies:

ADV_FSP.1 Informal Functional Specification

AGD_ADM Administrator Guidance

AGD_ADM.1 Administrator guidance

AGD_ADM.1.1D The developer shall provide administrator guidance addressed to system administrative personnel.

AGD_ADM.1.1C The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.

AGD_ADM.1.2C The administrator guidance shall describe how to administer the TOE in a secure manner.

AGD_ADM.1.3C The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.

AGD_ADM.1.4C The administrator guidance shall describe all assumptions regarding user behaviour that are relevant to secure operation of the TOE.

AGD_ADM.1.5C The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.

AGD_ADM.1.6C The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_ADM.1.7C The administrator guidance shall be consistent with all other documentation supplied for evaluation.

AGD_ADM.1.8C The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.

AGD_ADM.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

Dependencies:

ADV_FSP.1 Informal Functional Specification

AGD_USR User Guidance

AGD_USR.1 User guidance

AGD_USR.1.1D The developer shall provide user guidance.

AGD_USR.1.1C The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE.

AGD_USR.1.2C The user guidance shall describe the use of user-accessible security functions provided by the TOE.

AGD_USR.1.3C The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.

AGD_USR.1.4C The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behaviour found in the statement of TOE security environment.

AGD_USR.1.5C The user guidance shall be consistent with all other documentation supplied for evaluation.

AGD_USR.1.6C The user guidance shall describe all security requirements for the IT environment that are relevant to the user.

AGD_USR.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

Dependencies:

ADV_FSP.1 Informal Functional Specification

ALC_DVS Development Security

ALC_DVS.1 Identification of security measures

ALC_DVS.1.1D The developer shall produce development security documentation.

ALC_DVS.1.1C The development security documentation shall describe all the physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment.

ALC_DVS.1.2C The development security documentation shall provide evidence that these security measures are followed during the development and maintenance of the TOE.

ALC_DVS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ALC_DVS.1.2E The evaluator shall confirm that the security measures are being applied.

ATE_COV Coverage

ATE_COV.2 Analysis of coverage

ATE_COV.2.1D The developer shall provide an analysis of the test coverage.

ATE_COV.2.1C The analysis of the test coverage shall demonstrate the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.

ATE_COV.2.2C The analysis of the test coverage shall demonstrate that the correspondence between the TSF, as described in the functional specification and the tests identified in the test documentation, is complete.

ATE_COV.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

Dependencies:

ADV_FSP.1 Informal Functional Specification

ATE_FUN.1 Functional Testing

ATE_DPT Depth

ATE_DPT.1 Testing: high-level design

ATE_DPT.1.1D The developer shall provide the analysis of the depth of testing.

ATE_DPT.1.1C The depth analysis shall demonstrate that the tests identified in the test documentation are sufficient to demonstrate that the TSF operates in accordance with its high-level design.

ATE_DPT.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

Dependencies:

ADV_HLD.1 Descriptive High-level Design

ATE_FUN.1 Functional Testing

ATE_FUN Functional Tests

ATE_FUN.1 Functional testing

ATE_FUN.1.1D The developer shall test the TSF and document the results.

ATE_FUN.1.2D The developer shall provide test documentation.

ATE_FUN.1.1C The test documentation shall consist of test plans, test procedure descriptions, expected test results, and actual test results.

ATE_FUN.1.2C The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed.

ATE_FUN.1.3C The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests.

ATE_FUN.1.4C The expected test results shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.5C The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified.

ATE_FUN.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND Independent Testing

ATE_IND.2 Independent testing - sample

ATE_IND.2.1D The developer shall provide the TOE for testing.

ATE_IND.2.1C The TOE shall be suitable for testing.

ATE_IND.2.2C The developer shall provide an equivalent set of resources to those that were used in the developer’s functional testing of the TSF.

ATE_IND.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.2.2.E The evaluator shall test a subset of the TSF as appropriate to confirm that the TOE operates as specified.

ATE_IND.2.3E The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

Dependencies:

ADV_FSP.1 Informal Functional Specification

AGD_ADM.1 Administrator Guidance

AGD_USR.1 User Guidance

ATE_FUN.1 Functional Testing

AVA_MSU Misuse

AVA_MSU.1 Examination of guidance

AVA_MSU.1.1DThe developer shall provide guidance documentation.

AVA_MSU.1.1C The guidance documentation shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

AVA_MSU.1.2C The guidance documentation shall be complete, clear, consistent, and reasonable.

AVA_MSU.1.3C The guidance documentation shall list all assumptions about the intended environment.

AVA_MSU.1.4C The guidance documentation shall list all requirements for external security measures (including external procedural, physical and personnel controls).

AVA_MSU.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_MSU.1.2E The evaluator shall repeat all configuration and installation procedures to confirm that the TOE can be configured and used securely using only the supplied guidance documentation.

AVA_MSU.1.3E The evaluator shall determine that the use of the guidance documentation allows all insecure states to be detected.

Dependencies:

ADO_IGS.1 Installation, Generation, and Start-up Procedures

ADV_FSP.1 Informal Functional Specification

AGD_ADM.1 Administrator Guidance

AGD_USR.1 User Guidance

AVA_SOF Strength of TOE Security Functions

AVA_SOF.1 Strength of TOE security function evaluation

AVA_SOF.1.1D The developer shall perform a strength of TOE security function analysis for each mechanism identified in the ST as having a strength of TOE security function claim.

AVA_SOF.1.1C For each mechanism with a strength of TOE security function claim, the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST.

AVA_SOF.1.2C For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ST.

AVA_SOF.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_SOF.1.2E The evaluator shall confirm that the strength claims are correct.

Dependencies:

ADV_FSP.1 Informal Functional Specification

ADV_HLD.1 Descriptive High-level Design

AVA_VLA Vulnerability Analysis

AVA_VLA.1 Developer vulnerability analysis

AVA_VLA.1.1D The developer shall perform and document an analysis of the TOE deliverables, searching for obvious ways in which a user can violate the TSP.

AVA_VLA.1.2D The developer shall document the disposition of obvious vulnerabilities.

AVA_VLA.1.1C The documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE.

AVA_VLA.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_VLA.1.2E The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure obvious vulnerabilities have been addressed.

Dependencies:

ADV_FSP.1 Informal Functional Specification

ADV_HLD.1 Descriptive High-level Design

AGD_ADM.1 Administrator Guidance

AGD_USR.1 User Guidance

6. Rationale

This section presents the evidence used in the PP evaluation. This evidence supports the claims that the PP is a complete and cohesive set of requirements and that a conformant TOE would provide an effective set of IT security countermeasures within the security environment. The following sections will show these claims are valid.

Section 6.1 addresses Threat and Policy coverage by Objectives and Assumptions.

Section 6.2 addresses Objective coverage by TOE and environmental components.

Section 6.3 addresses the adequacy of the Assurance Requirements (EAL3+) chosen for this PP.

Section 6.4 addresses the minimum strength of function issues for this PP.

Section 6.5 addresses the comprehensive argument that the PP's IT requirements "form a mutually supportive and internally consistent whole."

6.1 Threat and Policy Coverage

This section contains a mapping table and individual arguments for each Policy and Threat that is covered. Table 5 lists either the Organizational Security Policy or Threat that requires coverage in the first column. Relevant and applicable Assumptions are listed in the second column. Objectives that cover each Policy and Threat, given the applicable Assumptions, are listed in the third column. Following this table are individual arguments for the coverage of each Policy and Threat.

Table 5 Threat and Policy Mapping to Security Objectives

Threats/Policies	Assumptions	Objectives
T.ATTACK_DATA	A.ADMIN A.BACK_UP A.MISUSE_DETECT	O.ADMIN O.ADMIN_SEPARATE O.ALARM O.BACK_UP O.HALT O.INTEGRITY O.PROPER_SPEC O.SELF_TEST O.TOE_AVAILABLE $\mathrm{O_{OU}}$.SPECIAL_PURPOSE

Threats/Policies	Assumptions	Objectives
T.BAD_ACCESS_INAPPROPRIATE	A.ADMIN A.BACK-UP A.CRYPTO_SUPPORT A.INFO_SECURITY_OFFICER A.MISUSE_DETECT A.POLICY_COMPLIANCE A.TRAIN A.USER_TRUSTED A_{OU}.PHYSICAL_SECURITY A_{RU}.PHYSICAL_SECURITY	O.ADMIN O.ALARM O.AUDIT O.BACK_UP O.PROPER_SPEC O.SECURITY_FUNCTION O.SELF_TEST O.SEPARATION O.TOE_AVAILABLE O.TOE_USER_ASSOCIATION O_{OU}.SPECIAL_PURPOSE
T.BAD_ACCESS_UNAUTHORISED	A.ADMIN A.BACK_UP A.MISUSE_DETECT A.LOGISTICS_SUPPORT A_{OU}.PHYSICAL_SECURITY A_{RU}.PHYSICAL_SECURITY	O.ADMIN O.ADMIN_SECURITY_REMOTE O.ALARM O.AUDIT O.BACK_UP O.CONFIDENTIALITY O.CONNECT O.CRYPTO_SUPPORT O.INTEGRITY O.PROTECT_ADDRESSES O.PROPER_SPEC O.REPLAY_PREVENT O.SECURE_STARTUP O.SECURITY_FUNCTION O.SELF_TEST O.SEPARATION O.TOE_AVAILABLE O.TOE_USER_ASSOCIATION O_{OU}.IDENTIFY_USER Oou.SPECIAL_PURPOSE O_{RU}.IDENTIFY_USER
T.BAD_ADMIN_ERROR	A.ADMIN A.BACK_UP A.INFO_SECURITY_OFFICER A.MISUSE_DETECT A.POLICY_COMPLIANCE	O.ADMIN_INTERFACE O.AUDIT O.ALARM O.BACK_UP O.HALT O.PROPER_SPEC O.TOE_AVAILABLE O_{OU}.SPECIAL_PURPOSE
T.BAD_ADMIN_HOSTILE	A.ADMIN A.BACK_UP A.INFO_SECURITY_OFFICER A.MISUSE_DETECT A.POLICY_COMPLIANCE A.LOGISTICS_SUPPORT	None – assumed away by the assumptions already.
T.BAD_AUDIT_OVERFLOW	A.ADMIN	O.ALARM O.AUDIT O.PROPER_SPEC O.SELF_TEST
T.BAD_AUDIT_SEQUENCE	None	O.AUDIT O.PROPER_SPEC

Threats/Policies	Assumptions	Objectives
T.BAD_AUDIT_UNDETECTED	A.MISUSE_DETECT	O.ALARM O.AUDIT O.PROPER_SPEC
T.BAD_AUDIT_UNTRACEABLE	A.ADMIN A.BACK_UP A.MISUSE_DETECT	O.ADMIN_SECURITY_REMOTE O.ALARM O.AUDIT O.BACK_UP O.PROTECT_ADDRESSES O.PROPER_SPEC O.SELF_TEST O_{OU}.IDENTIFY_USER O_{RU}.IDENTIFY_USER
T.BAD_DESIGN_BYPASS	A.DESIGN_BYPASS	None – taken care of by assumption.
T.BAD_DESIGN_COMPLEXITY	A.BACK_UP	O.ADMIN O.ADMIN_INTERFACE O.BACK_UP O.PROPER_SPEC
T.BAD_DESIGN_EXTERNAL	A.BACK_UP A.LOGISTICS_SUPPORT A.MISUSE_DETECT A_{OU}.PHYSICAL_SECURITY A_{RU}.PHYSICAL_SECURITY	O.ALARM O.BACK_UP O.PROPER_SPEC O.SECURE_STARTUP
T.BAD_DESIGN_SECURITY_ FUNCTION_CORRUPTION	A_BACK_UP A.MISUSE_DETECT A.USER_TRUSTED A_{OU}.PHYSICAL_SECURITY A_{RU}.PHYSICAL_SECURITY	O.BACK_UP O.PROPER_SPEC O.SECURITY_FUNCTION
T.BAD_PROCEDURES	A.BACK_UP A.INFO_SECURITY_OFFICER A.MISUSE_DETECT A.POLICY_COMPLIANCE A.USER_TRUSTED	O.ADMIN_INTERFACE O.ALARM O.BACK_UP O.SECURE_STARTUP O.SECURITY_FUNCTION O.SELF_TEST O.TOE_AVAILABLE
T.CRYPTANALYTIC	A.CRYPTANALYTIC	O.PROPER_SPEC
T.COVERT_CHANNELS	A.MISUSE_DETECT A.USER_TRUSTED	O.CONFIDENTIALITY O.PROPER_SPEC O.SECURITY_FUNCTION
T.MALFUNCTION	A.BACK_UP A.LOGISTICS_SUPPORT	O.ALARM O.AUDIT O.BACK_UP O.PROPER_SPEC O.RELIABLE O.SECURE_STARTUP O.SELF_TEST O.SEPARATION O.TOE_AVAILABLE O_{OU}.IDENTIFY_USER O_{RU}.IDENTIFY_USER

Threats/Policies	Assumptions	Objectives
T.MASQUERADE_BYPASS	A.MISUSE_DETECT	O.ADMIN_SECURITY_REMOTE O.ALARM O.AUDIT O.CONFIDENTIALITY O.CONNECT O.CRYPTO_SUPPORT O.INTEGRITY O.PROTECT_ADDRESSES O.PROPER_SPEC O.SELF_TEST O_{OU}.IDENTIFY_USER O_{RU}.IDENTIFY_USER
T.MASQUERADE_HIJACK	A.MISUSE_DETECT	O.ADMIN_SECURITY_REMOTE O.ALARM O.AUDIT O.CONFIDENTIALITY O.CONNECT O.CRYPTO_SUPPORT O.INTEGRITY O.PROPER_SPEC O.PROTECT_ADDRESSES O.SELF_TEST O_{OU}.IDENTIFY_USER O_{RU}.IDENTIFY_USER
T.MULTIPLE_PATHS	A.ADMIN A.INFO_SECURITY_OFFICER A.POLICY_COMPLIANCE	None
T.PHYSICAL_SECURITY	A.ADMIN A.BACK_UP A.INFO_SECURITY_OFFICER A.POLICY_COMPLIANCE A.THREAT_LEVEL A.TRAIN	O.AUDIT O.BACK_UP O.HALT O.TOE_USER_ASSOCIATION O_{OU}.IDENTIFY_USER O_{RU}.IDENTIFY_USER
T.POLICY_INTERPRETATION	A.ADMIN A.CRYPTO_SUPPORT A.INFO_SECURITY_OFFICER A.POLICY_COMPLIANCE	O.ADMIN_INTERFACE
T.REPUDIATION	A.ADMIN A.MISUSE_DETECT	O.ADMIN_SECURITY_REMOTE O.AUDIT O.CRYPTO_SUPPORT O.PROPER_SPEC O_{OU}.IDENTIFY_USER O_{RU}.IDENTIFY_USER
T.TEMPEST	A.TEMPEST	None
T.TRAFFIC_ANALYSIS	None	O.PROPER_SPEC O.PROTECT_ADDRESSES
T.TRANSMISSION_ERRORS	A.MISUSE_DETECT	O.ALARM O.INTEGRITY O.PROPER_SPEC O.TOE_AVAILABLE
T.UNAVAILABLE	A.AVAILABLE	None

Threats/Policies	Assumptions	Objectives
P.ACCOUNT	A.ADMIN A.MISUSE_DETECT	O.ADMIN O.AUDIT O.CRYPTO_SUPPORT O.PROPER_SPEC O_{OU}.IDENTIFY_USER
P.ADMIN_SECURITY_ RESTRICTED	A.MISUSE_DETECT	O.ADMIN O.ALARM O.AUDIT O.CRYPTO_SUPPORT O.PROPER_SPEC O.ADMIN_SECURITY_REMOTE O_{OU}.IDENTIFY_USER O_{RU}.IDENTIFY_USER
P.AUDIT_REVIEW	A.INFO_SECURITY_OFFICER A.POLICY_COMPLIANCE	O.AUDIT
P.AVAILABLE	A.ADMIN A.AVAILABLE A.INFO_SECURITY _OFFICER A.LOGISTICS_SUPPORT A.MISUSE_DETECT	O.ADMIN_INTERFACE O.ALARM O_{OU}.IDENTIFY_USER O_{RU}.IDENTIFY_USER
P.COMPLY	A.INFO_SECURITY_OFFICER A.MISUSE_DETECT A.POLICY_COMPLIANCE A_{OU}.PHYSICAL SECURITY A_{RU}.PHYSICAL_SECURITY	O.CONFIDENTIALITY O.INTEGRITY
P.DEFEND	A.ADMIN A.AVAILABLE A.INFO_SECURITY_OFFICER A.MISUSE_DETECT A.TRAIN	O.ALARM O.CRYPTO_SUPPORT O.HALT O.PROPER_SPEC O.SECURITY_FUNCTION O.SELF_TEST O.TOE_AVAILABLE O.TOE_USER_ASSOCIATION O_{OU}.IDENTIFY_USER O_{RU}.IDENTIFY_USER
P.DISTRIBUTION	A.INFO_SECURITY_OFFICER A.POLICY_COMPLIANCE	O.ADMIN O.ADMIN_INTERFACE

Threats/Policies	Assumptions	Objectives
P.DUE_CARE	A.ADMIN A.BACK_UP A.CRYPTO_SUPPORT A.DESIGN_BYPASS A.INFO_SECURITY_OFFICER A.LOGISTICS_SUPPORT A.MISUSE_DETECT A.POLICY_COMPLIANCE A.THREAT_LEVEL A_{OU}.PHYSICAL_SECURITY A_{RU}.PHYSICAL_SECURITY	O.ADMIN O.ADMIN_INTERFACE O.ADMIN_SECURITY_REMOTE O.ADMIN_SEPARATE O.ALARM O.AUDIT O.BACK_UP O.CONFIDENTIALITY O.CONNECT O.CRYPTO_SUPPORT O.HALT O.INTEGRITY O.PROPER_SPEC O.PROTECT_ADDRESS O.RELIABLE O.REPLAY_PREVENT O.SECURE_STARTUP O.SECURITY_FUNCTION O.SELF_TEST O.SEPARATION O.TOE_AVAILABLE O.TOE_USER_ASSOCIATION O_{OU}.IDENTIFY_USER O_{OU}.SPECIAL_PURPOSE O_{RU}.IDENTIFY_USER
P.LABEL	A.INFO_SECURITY_OFFICER A.POLICY_COMPLIANCE	None
P.MANAGE	A.ADMIN A.INFO_SECURITY_OFFICER A.POLICY_COMPLIANCE	O.ADMIN O.ADMIN_INTERFACE O.ADMIN_SECURITY_REMOTE O.AUDIT O.SELF_TEST
P.PERSONNEL_TRUST_COI	A.USER_TRUSTED	O.CRYPTO_SUPPORT
P.PERSONNEL_TRUST_MINIMUM	A.USER_TRUSTED	O.CRYPTO_SUPPORT
P.PROCEDURES	A.INFO_SECURITY_OFFICER A.POLICY_COMPLIANCE	O.ADMIN_INTERFACE O.TOE_AVAILABLE
P.PROTECT	A.ADMIN A.CRYPTO_SUPPORT A.INFO_SECURITY_OFFICER A.MISUSE_DETECT A.TRAIN	O.ALARM O.CONFIDENTIALITY O.CRYPTO_SUPPORT O.HALT O.INTEGRITY O.PROTECT_ADDRESS O.SECURITY_FUNCTION O.SELF_TEST
P.RECIPIENTS	A.ADMIN A.INFO_SECURITY_OFFICER A.MISUSE_DETECT A.POLICY_COMPLIANCE	O.ADMIN O.AUDIT O.ADMIN_INTERFACE O.ALARM O.CONNECT O.HALT O.PROTECT_ADDRESS O.TOE_USER_ASSOCIATION O_{OU}.IDENTIFY_USER O_{RU}.IDENTIFY_USER

Threats/Policies	Assumptions	Objectives
P.RELEASE_NON-SENSITIVE	A.INFO_SECURITY_OFFICER A.POLICY_COMPLIANCE	O.CONFIDENTIALITY O.INTEGRITY
P.REMOTE_SECURITY_ADMIN		O.ADMIN O.ADMIN_SECURITY_REMOTE O.CRYPTO_SUPPORT O.PROPER_SPEC O$_{OU}$.IDENTIFY_USER O$_{RU}$.IDENTIFY_USER
P.TOE_USAGE	A.INFO_SECURITY_OFFICER A.MISUSE_DETECT A.POLICY_COMPLIANCE A.USER_TRUSTED	O.ADMIN_INTERFACE O.CONNECT O.PROPER_SPEC O.SECURITY_FUNCTION O.TOE_USER_ASSOCIATION O$_{OU}$.IDENTIFY_USER O$_{RU}$.IDENTIFY_USER
P.TRAIN	A.TRAIN	None
P.TSE_CONNECTIONS	A.ADMIN A.MISUSE_DETECTION A.POLICY_COMPLIANCE A$_{OU}$.PHYSICAL_SECURITY A$_{RU}$.PHYSICAL_SECURITY	O.TOE_USER_ASSOCIATION O$_{OU}$.IDENTIFY_USER O$_{RU}$.IDENTIFY_USER
P.USAGE	A.INFO_SECURITY_OFFICER A.POLICY_COMPLIANCE	O.PROPER_SPEC O.TOE_USER_ASSOCIATION O$_{OU}$.IDENTIFY_USER O$_{RU}$.IDENTIFY_USER

T.ATTACK_DATA - The TOE will encounter data that may contain malicious code. An Authorized User or Unauthorized Agent may use malicious code to attempt to disrupt site security operations or the TOE itself.

RATIONALE: **A.ADMIN** helps to control the problem of malicious code by having full-time administrators, (one of whom specializes in security issues,) who monitor the system at the operational user site. Also, the administrators configure and manage the MD system. Splitting administrative responsibility increases the probability that insecurities and accidents will be detected before problems occur. Splitting responsibilities helps considerably, even if one of the administrators goes bad. This threat and assumption drives the objective **O.ADMIN**, which provides for administrators to manage the system, for the splitting of roles between administrators, and for the protection against one bad administrator. Note that nothing helps, if both administrators go bad and collaborate.

A.BACK_UP helps authorized remote site users and OU site System and Security Administrators back up the system periodically so that it can be restored if a malicious code attack is successful.

A.MISUSE_DETECT is included so that the OU site TOE is not encumbered with all the error and alarm checking processes within its boundary given that an adversary launches a malicious code attack. The TOE collects fault data and sends it to a mechanism in the MD environment that will perform misuse checking. This eases the TOEs processing burden. This assumption gave rise to the objectives **O.ALARM, O.HALT** and **O.SELF_TEST**, all of which work in conjunction with some sort of Misuse Detection system (MD) and/or directly trigger alarms within the TOE.

The objective **O.BACK_UP** is included so that the TOE has an automated back up system built into it, which is easy for the authorized remote user and System or Security Administrator to use.

The Objective **$\mathbf{O_{OU}}$.SPECIAL_PURPOSE** minimizes the possibility that malicious code can affect the OU TOE. By creating a TOE that cannot be object code changed by the customer and will not allow general purpose programs to run, we are more confident that malicious code will not corrupt the functionality of the TOE. This is not to say that malicious code cannot flow through the TOE into the environment. However, we assume further that the environment contains misuse detection software (**A.MISUSE_DETECT**) which will prevent the effect of such a condition. Given that the TOE is a special purpose device with relatively static object code, the designers of the TOE would be wise to provide automatic self-testing. One function of self-testing is to review its code and ensure no corruption has occurred. Thus, we included **O.SELF_TEST** as an objective in both site environments.

Finally, the TOE's job is to receive data, and transmit that data to another TOE securely. It must do these functions even if attacked by an adversary using malicious data to corrupt the TOE. The TOE must protect itself from code trying to alter the original data it means to protect, must protect itself from a denial of service attack, and must protect the data from inadvertent disclosure. This gives rise to the three basic security objectives: **O.INTEGRITY**, **O.PROPER_SPEC**, and **O.TOE_AVAILABLE**. All three are applicable regardless of the site from which it operates.

T.BAD_ACCESS_INAPPROPRIATE - Authorized Users may intentionally or unintentionally access or modify information, utilize resources for which they are not approved, or release sensitive data to unprivileged parties.

RATIONALE: A.ADMIN establishes that there are System and Security Administrators. These administrators can help to avert compromise or damage caused by Authorized Users whether intentional or accidental.

A.CRYPTO_SUPPORT says that a cryptographic support infrastructure is available to provide elements needed to implement cryptography for personal accountability.

A.INFO_SECURITY_OFFICER is an assumption that says a person is assigned to write and maintain site security policy and procedures that are followed by the System and Security Administrators who assist in controlling damage caused by Authorized Users.

A.MISUSE_DETECT helps to mitigate the threat because it says that misuse detection mechanisms are in place looking for potential system misuse.

A.POLICY_COMPLIANCE also helps to counter the threat by assuming that Authorized Users and System and Security Administrators are competent and will typically, accurately carry out the site security policy. The implication is they will typically not make mistakes. However, there remains residual risk because the assumption is not absolute, but is mitigated somewhat by having split administrative duties.

A.TRAIN can help to prevent Authorized Users from making unintentional mistakes like releasing sensitive data to unprivileged parties. It assumes that appropriate training is provided.

A.USER_TRUSTED helps somewhat to counter the threat by assuming that Authorized Users are trusted, mainly because adequate checks on their past have been made before hiring them. However, it also says that they sometimes cannot be trusted, leaving the threat still viable.

A.BACK_UP helps to control damage caused by Authorized Users by maintaining a record of the System State at a point in the not too distant past.

O.BACK_UP is included so that the TOE has an automated back up system built into it, which is easy for the RU site user and the System or Security Administrator to use.

A_{OU}.PHYSICAL_SECURITY assumes that the Operational User site has adequate physical security consisting of e.g. physical walls, locks, guards, alarms, and surveillance cameras. It is assumed these measures are good enough to restrict physical access to the TOE, the MD and other security devices to only System and Security Administrators.

At a RU site, **A_{RU}.PHYSICAL_SECURITY** assumes that physical security is typically less robust than at an OU site. Consequently, there is additional burden placed on procedural controls and perhaps other mechanisms included within the TSE which will insure that stored data is secured by techniques such as physical secure storage of media or encryption when left unattended by the RU site AU. These additional objectives are captured in OE_{RU}.PHYSICAL_SECURITY.

O.ADMIN helps counter that portion of the threat directed at the TOE by requiring the TOE to have its security functions managed and accessed only by System and Security Administrators.

O.ALARM helps counter the threat by requiring the TOE_{OU} to detect violations of the site security policy that relate to the TOE_{OU} and notify the System and Security Administrators. It also helps focus the developer on providing some mechanisms to alarm remote users that the TOE_{RU} has experienced an inappropriate access.

O.AUDIT requires the TOE_{OU} to perform auditing so that people can be held accountable for their actions. This provides some deterrence, which aids in countering the threat.

O.BACK_UP is included so that the TOE_{OU} has an automated back up system built into it, which is easy for the System or Security Administrator to use. Also**, O.BACK_UP** drives a requirement for the TOE_{RU} to incorporate means, which allow the remote user to perform manual back ups.

O.PROPER_SPEC is very important to making the TOE resistant to the threat. It says that the TOE should be well designed and contain strong security protections.

O.SECURITY_FUNCTION reduces the threat by minimizing the extent of control an Authorized User has.

O.SELF_TEST is important because it requires the TOE to check the health of its security functions in case Authorized Users have purposefully or accidentally altered its security functionality.

O.SEPARATION can reduce the threat of inappropriate access to private data by insisting the security designers provide for the proper separation of sessions and data between and among users. Session and data separation will minimize the security impact of the threat of various types of bad access.

O.TOE_AVAILABLE can reduce the threat resulting in denial of service by requiring the TOE to be resistant to these types of attacks.

O.TOE_USER_ASSOCIATION is important in preventing the threat of inappropriate access, because it requires strong, logical identification, authentication and verification of users between the transmitting and receiving TOEs. Therefore, only authorized personnel should be able to gain access.

$\mathbf{O}_{\mathbf{OU}}$.SPECIAL_PURPOSE also aids in countering the threat by reducing the number and type of possible attacks to the TOE_{OU}. It does this by limiting what code can be executed

T.BAD_ACCESS_UNAUTHORISED - Unauthorized Agents may intentionally access or modify information, or utilize resources for which they are not approved.

RATIONALE: This threat differs from the previous threat in that it deals with an Agent with bad intentions rather than a user who has good intentions, but errs. Many of the assumptions and all the objectives we discussed in the previous threat remain valid to mitigate risk relative to this threat.

The assumptions **A.ADMIN, A.BACK_UP, A.MISUSE_DETECT**, **$\mathbf{A}_{\mathbf{RU}}$.PHYSICAL_SECURITY** and **$\mathbf{A}_{\mathbf{OU}}$.PHYSICAL_SECURITY** would obviously help mitigate this threat as well as they did in the previous one. In addition, the security objectives called out for **T.BAD_ACCESS_INAPPROPRIATE** are useful for **T.BAD_ACCESS_UNAUTHORISED**. Objectives such as **O.AUDIT, O.BACK_UP**,

O.SELF_TEST are important as well relative to this threat. Having proper administration, special purpose functionality in your TOE hardware and software, and the other objectives listed for **T.BAD_ACCESS_INAPPROPRIATE** protects against this threat.

A.LOGISTICS_SUPPORT helps in that, if an Agent is successful in an attack that actually causes physical harm to the TOE or TSE, by having a supply of spares that your Administrators can apply mitigates the risk of denial of service.

O.ADMIN and **O.ADMIN_SECURITY_REMOTE** ensure that administrators are assigned and all available security precautions to protect the important role of OU and RU site administration are performed.

O.CONFIDENTIALITY will ensure that an Agent will not be able to gain access to unprotected information anywhere between users.

O.CONNECT helps in that it requires proper identification between users prior to the TOEs connecting and communicating.

O.CRYPTO_SUPPORT is important in insuring the establishment and integrity of vital security parameters such as ACLs and keys so that inappropriate personnel are locked out from using the TOE and its environment.

O_{OU}.IDENTIFY_USER is important so that user identification is continuously checked during the TOE operation and an alarm triggered, if this check fails. This check is at the IP address level and authenticated user password, which is as granular as we could require based on how VPNs are currently constructed.

O_{RU}.IDENTIFY_USER at a RU site also insures that the authorized remote user is authenticated based on their hardware token and password.

O.INTEGRITY will ensure that an Agent has not modified sensitive data. By performing well-established integrity functions, the TOEs will be able to check that the original information is unaltered.

O.PROTECT_ADDRESSES is also vital in that the attacker of an OU site not be allowed to substitute additional or replacement addresses or destroy addresses.

O.REPLAY_PREVENT drives requirements for the TOE to be able to identify attempts by unauthorized agents (UAs) to masquerade as AUs and gain unauthorized access.

O.SECURE_STARTUP ensures that care is taken to provide initial secure start-up and resumption of service in case of failure. Often attacks occur during the start-up process after these two events.

T.BAD_ADMIN_ERROR - System or Security Administrators may unintentionally make a security relevant error that results in inappropriate access or modification of information, or inappropriate utilization of resources.

RATIONALE: A.ADMIN establishes that there are two administrators. Having two administrators may help to avert compromise or damage caused by one of the administrators making an error simply because the administrator may notice the other's error.

A.INFO_SECURITY_OFFICER is an assumption that that says a person is assigned to write and maintain site security policy and procedures. Having these policies and procedures written for the System and Security Administrators to follow can aid in reducing errors that the administrators may make.

A.MISUSE_DETECT helps to mitigate the threat because it says that misuse detection mechanisms are in place looking for potential misuse that can be in the form of human errors caused by the administrators.

A.POLICY_COMPLIANCE helps somewhat to counter the threat by if the administrators are competent. The more competent they are the fewer errors they are likely to make.

A. BACK_UP helps to control damage caused by a System or Security Administrator's error at an OU site, or AU error at an RU site, by maintaining a record of the system state at a point in the not too distant past.

O.ADMIN_INTERFACE reduces the threat by requiring the TOE to have a user-friendly interface for the administrators so that errors are minimized.

O.ALARM helps to counter the threat by requiring the TOE_{OU} to detect violations of the site security policy (which could be caused by administrator error) that relate to the TOE_{OU} and notify the System and Security Administrators. It also helps focus the developer on providing mechanisms to alarm remote users that the TOE_{RU} has experienced and administrative error.

O.AUDIT requires the TOE_{OU} to perform auditing so that people can be held accountable. If System and Security Administrators know that they will be held accountable for their errors they are likely to make fewer errors.

O.BACK_UP is necessary to allow for recovery of the TOE functions in case either administrator or remote user makes an error that affects the TOE functionality.

O.HALT helps to mitigate the impact of the threat because it requires the TOE to stop processing and default to a secure state whenever an insecure operation is detected. The insecure operation could be caused by an administrative error.

O.PROPER_SPEC can help to mitigate the threat because it requires the TOE to be well designed and contain strong security protections, which should include design features that attempt to preclude operator errors.

O.TOE_AVAILABLE helps a little in countering the threat by requiring the TOE to be resistant to denial of service attacks.

O$_{OU}$.SPECIAL_PURPOSE aids in countering the threat by reducing the number of possible errors that can be made. It does this by requiring that extraneous software not be allowed to run on the TOE.

T.BAD_ADMIN_HOSTILE - The System or Security Administrator *intentionally* takes a security relevant action that results in inappropriate access or modification of information, or inappropriate utilization of resources.

RATIONALE: The administrative function has become a very powerful and vital one for any organization. An organization that puts the entire administrative burden in the hands of one person is asking for trouble. To do so puts the entire operation at risk. The threat that one of your administrators becomes hostile is undoubtedly one of the worst events any organization can experience. This threat is exceptionally difficult to defend against and, therefore, most security approaches assume thorough enough background checks or using such mechanisms as polygraph exams on their key people will mitigate the problem. We decided that the only way to defend effectively and efficiently against this increasingly likely threat is to split the administrative functions into two parts, a systems and a security part. There remains overlap between these two job functions and they should be defined such that both administrators must become hostile in order for the good one not to realize the hostile one had gone bad.

A.ADMIN assumes that administrators exist in the environment and are normally trustworthy. In addition it is assumed that the organization desires to implement the checks and balances provided by split administrative duties.

In addition, **A.MISUSE_DETECT** assumes having a well-constructed MD system, which will help System, and Security Administrators detect hostile actions and terminate them before they are successful.

Two assumptions we made assume away the some of the threat of this attack. We assume that administrators normally follow all the policy laid out by the Site Security Officer (**A.INFO_SECURITY_OFFICER** and **A.POLICY_COMPLIANCE**).

Having an ample and protected supply of spare parts available for good maintenance and administrative personnel is a good idea in the event that the bad administrator attacked various physical parts of the TOE or the TOE environment (**A.LOGISTICS_SUPPORT**). In modern computer systems the administrators are expected to perform first-line maintenance.

A.BACK_UP assumes that backed up TOE files and configuration parameters exist to restore the TOE to a semblance of sanity in the event that either a hostile System or Security Administrator launched an attack

T.BAD_AUDIT_OVERFLOW - Legitimate audit records may be lost due to excessive volume of records.

RATIONALE: A.ADMIN establishes that there are administrators. These administrators are responsible to see that audit overflows do not occur, therefore, the threat may be partially mitigated by having alert administrators.

O.ALARM states that when audit record overflow conditions occur the TOE must be alerted. The TOE must shut down its operation until the overflow condition is corrected. Typically, a mechanism in the TSE will alert the TOE of this condition, while at the same time alerting the Security Administrator.

O.AUDIT provides the requirement for the TOE to report out auditable events. The reporting would be to the Misuse Detection system.

O.PROPER_SPEC requires that the TOE be adequately designed which would preclude such things as audit data being lost, disrupted, or altered as it is sensed and reported out of the TOE.

O.SELF_TEST says that the TOE must perform self-tests of its security functions which helps ensure that the TOE is working properly, including the audit reporting function.

T.BAD_AUDIT_SEQUENCE - Legitimate audit records may not be attributed to time of occurrence resulting in inconclusive audit analysis.

RATIONALE: The threat of an audit trail sequence error makes post attack analysis difficult to impossible to perform. A sequence error can occur because of a poorly designed audit collection routine or because a person in the environment changed the audit record. Two objectives handle these concerns. **O.AUDIT** deals with the problem of people altering the audit records, while **O.PROPER_SPEC** deals with the improperly designed code that might not record timing data properly. The remote user has limited auditing functionality, so the risk of this threat in the remote environment is higher than at the operational user site. For this reason, more care is taken to monitor who the remote users are and for what purpose they need remote access.

T.BAD_AUDIT_UNDETECTED - Intentional or unintentional access or modification of information or utilization of resources may go undetected whether performed by Authorized Users, System or Security Administrators or Unauthorized Agents

RATIONALE: **A.MISUSE_DETECT** assumes that there is a properly working Misuse Detection system taking audit data from the TOE, storing it and performing analysis thereby aiding in countering the threat.

O.ALARM is the objective that insists alarm mechanisms exist that are triggered when the Misuse Detection system indicates that something went amiss within the auditing process.

O.AUDIT is the objective that auditing is easily understood and protected. Such protection, if designed properly, will prevent easy modification or corruption of audit records.

O.PROPER_SPEC is the objective that the audit mechanism be well specified and designed from the start so that this threat is mitigated.

T.BAD_AUDIT_UNTRACEABLE - Accesses or modification of information or utilization of resources by Unauthorized Agents may not be traceable to their source.

RATIONALE: The threats to audit records make post attack analysis difficult to impossible to perform. The Security Administrator and Information Security Officer must limit who has access to audit information and analyze the mechanisms themselves to ensure they are designed and functioning properly. We made three assumptions relative to this threat.

A.ADMIN articulates the assumption that you have System and Security Administrators with well-defined and somewhat overlapping tasks.

A.MISUSE_DETECT assumes the system has a well designed MD system in place which aids in making reliable conclusions concerning who performed what actions and when.

A. BACK_UP assumes you have an environment where system back up procedures are faithfully performed.

O.ADMIN_SECURITY_REMOTE states that if you permit remote administration, you must take special care to perform it securely and, therefore must provide for a TOE-to-TOE secure path. This provides source authentication.

O.ALARM states that when violations occur the TOE will be able to alarm the proper mechanisms that will perform pre-arranged alarming.

O.AUDIT is the basic objective that auditing is designed in well between the TOE and the MD system.

O.BACK_UP is necessary to compare version of the TOE's files and its configuration parameters before and after a suspected security event such as this.

O$_{OU}$.IDENTIFY_USER is the objective that leads to requirements that only authorized users may access the TOE and that access will be performed in a proper manner.

O$_{RU}$.IDENTIFY_USER at a RU site also insures that the authorized remote user is authenticated based on their hardware token and password.

O.PROPER_SPEC specifies that the TOE has been properly designed and implemented, thus reducing the possibility of this attack being successful.

O.PROTECT_ADDRESSES leads to TOE requirements that ensure the confidentiality and integrity of transmitting and receiving addresses of authorized users at OU sites.

O.SELF_TEST is the objective that the TOE has been designed with the ability to check itself occasionally to insure it has not been altered.

T.BAD_DESIGN_BYPASS - The design or architecture of the system allows security mechanisms to be bypassed and this bypass function (typically used to communicate with lessor privileged users) may be inappropriately utilized. Either the bypass technique or function may be embedded within the TOE (e.g. RU site TOE) or external to it located within a shared boundary security functional area (e.g. OU site Boundary Security Function).

RATIONALE: The assumption **A.DESIGN_BYPASS** assumes away this threat for the TOE but not the TSE. It reads, “Any bypass of the TOE will be performed outside the TOE but within the TSE. At an OU site, bypass functions will be performed within a physically controlled boundary protection area, which is accessible to only System and Security Administrators. At an RU site, bypass functions, if required, will be performed utilizing periods processing techniques”

T.BAD_DESIGN_COMPLEXITY - Authorized Users, System or Security Administrators, may accidentally modify security functions, because of the complexity of the design or operation resulting in a violation of the site security policy.

RATIONALE: The complexity of modern computer systems increases the possibility of Authorized Users, and Systems and Security Administrators making mistakes that result in security violations.

The assumption **A.BACK_UP** mitigates, but does not eliminate, this threat by reminding the organization that implementing robust back up procedures will be invaluable when the system must be restored.

The threat of system complexity leads to the need for competent system and security administration at the Operational User Site. Hence, **O.ADMIN** is a logical objective.

Vendors should provide user-friendly interfaces for present day systems. Ease of use translates into less security related errors. Hence, we included **O.ADMIN_INTERFACE**.

O.BACK_UP sets up an objective for the vendor to incorporate back up procedures and mechanisms that are easy to implement.

The same rationale gives rise to the objective that security mechanisms be properly specified, designed and implemented (**O.PROPER_SPEC**). By doing so, there is much less risk of causing security relevant errors because of complex design.

T.BAD_DESIGN_EXTERNAL - System design is insufficient to prevent random conditions external to the TSE from resulting in detrimental affects. Examples are lightening storms and human error.

RATIONALE: **A.MISUE_DETECT** assumes that a system is in place to monitor for "bad" things happening. This has a chance of helping to detect that something bad has happened which affected the TOE's operation and allow for notification and corrective actions.

A.LOGISTICS_SUPPORT helps to get the system back on line after a damaging external event by assuming there are hot spares available.

A.BACK_UP helps to control damage caused by an external event by maintaining a record of the TOE's files and configuration parameters at a point in the not too distant past.

A_{OU}. PHYSICAL_SECURITY assumes the TOE_{OU} is in a physically controlled boundary protection area. By assuming this, a portion of the external threat is mitigated, such as those arising from some close–in, physical causes.

At a RU site, **A_{RU}.PHYSICAL_SECURITY** assumes that physical security is typically less robust than at an OU site. Consequently, there is additional burden placed on procedural controls and perhaps other mechanisms included within the TSE which will insure that stored data is secured by techniques such as physical secure storage of media or encryption when left unattended by the RU site AU. These additional objectives are captured in OE_{RU}.PHYSICAL_SECURITY.

O.ALARM can help to minimize the impact of an external event causing a detrimental affect by alerting the System or Security Administrators or remote user that something is wrong.

O.BACK_UP provides for reconstitution of the TOE at both OU and RU sites after a detrimental event.

O.PROPER_SPEC requires that the TOE be well designed so that it minimizes the types and numbers of external detrimental events that are possible.

O.SECURE_STARTUP requires that the TOE not be forced to an insecure state by these detrimental external events.

T.BAD_DESIGN_SECURITY_FUNCTION_CORRUPTION - System design is insufficient to prevent Unauthorized Agents from modifying security critical functions within the TSE.

RATIONALE: If security is not taken into account during the development of your computer system, often system design is not robust enough in a security sense to defend system assets from an attack. Because we rely on off-the-shelf, commercial systems as the base from which we develop systems, we are limited in the protection we can provide after the fact.

A.BACK_UP is the assumption that even in the event that there are successful attacks which the system designers did not anticipate, a back up capability exists that will enable the properly trained personnel to restore the system.

A.MISUSE_DETECT is the assumption that we will purchase and use wisely a variety of applications in the TSE that will look for attacks and warn us when they are on going or discover they have occurred. Often these applications provide good protection.

A.USER_TRUSTED is the assumption that usually your inside personnel are trustworthy. However, there are times that even after extensive checks, people disappoint and betray that trust. This is the reason we advise mechanisms such as intrusion detection and other misuse applications.

A_{OU}.PHYSICAL_SECURITY is the assumption that at least in the Operational User site, you can secure your physical boundary and limit the accessibility to authorized administrators. It makes good sense to limit your security assets to very few, trusted people.

At a RU site, **A_{RU}.PHYSICAL_SECURITY** assumes that physical security is typically less robust than at an OU site. Consequently, there is additional burden placed on procedural controls and perhaps other mechanisms included within the TSE which will insure that stored data is secured by techniques such as physical secure storage of media or encryption when left unattended by the RU site AU. These additional objectives are captured in OE_{RU}.PHYSICAL_SECURITY.

O.BACK_UP is a vital, automatic security service that helps System and Security Administrators and RU site AUs restore services in case of a successful attack.

O.PROPER_SPEC is the objective to design security into your system that at least matches the risk you are willing to assume. It states that cryptographic and other means will be carefully considered, integrated and applied as the system is developed and fielded. We have specified many requirements to satisfy this objective in the Protection Profile.

O.SECURITY_FUNCTION is the wise objective to limit the control an individual user has on the TOE security functionality to a minimum.

T.BAD_PROCEDURES - Operational procedures are either inadequate or are not followed, resulting in unapproved access or modification of information, or inappropriate utilization of resources. Examples are: Storage media is allowed to age rendering it unreadable; Virus checking capability is insufficient resulting in loss or compromise of data; Inadequate TOE configuration data back up procedures or mechanisms result in the inability to restore the TOE to normal operation.

RATIONALE: Inadequate procedures or procedures that are not followed are a major source of insecurities. The assumption **A_BACK_UP** assumes that the bad procedures involved in this threat do not include back up procedures. Thus, a good back up version of the TOE can restore operations to a point in the not too distant past.

The assumption **A.POLICY_COMPLIANCE** assumes away policy guidance that is not recorded as procedures. It states that those users and administrators who are charged with following procedures will do so as well as can be expected. It does not assume they are perfect. This still leaves the threat resulting from inadequate or no procedures where there should be some; and the threat of procedures not being followed because of ignorance or mistake.

A.INFO_SECURITY_OFFICER closes some of the threats discussed in the previous paragraph. It assumes that the site has a security-proficient person who spends time and ample energy working on site security policies and procedures, and implementation and inspection issues. Also, this person will be cognizant of security issues that arise between sites.

A.MISUSE_DETECT assumes that the site has a Misuse Detection system in place that alerts administrators that security relevant, procedural events have taken place.

A.USER_TRUSTED assumes that normally users are trustworthy. This assumption helps mitigate this threat. We did not assume that users are always trustworthy, competent, or will always follow procedures. Our objectives reflect this pragmatic approach to Authorized Users.

O.ADMIN_INTERFACE is the important objective to present security relevant event data to the administrators of the system in a manner that is user-friendly. Often, auditable data is presented in a way that does not alert the proper administrator in a way that he will understand.

O.ALARM is the objective to have a robust alarm system that keeps administrators informed concerning as many security relevant events as possible.

O.BACK_UP is an automatic security service that must be designed into the TOE to enable System and Security Administrators to restore TOE services to a previous good state in the event of a failure or successful attack.

O.SECURE_STARTUP insists that upon initial start-up or when recovering, the designers of the TOE were careful about starting or leaving the TOE in a secure state. This objective avoids saddling administrators with needless start-up or recovery procedures.

O.SECURITY_FUNCTION is the wise objective to limit the *control* an individual user has on the TOE security functionality to a minimum. One procedure that all sites would want to maintain is not allowing users and administrators access to the cryptographic functionality of the TOE.

O.SELF_TEST is the objective that the TOE has been designed with the ability to check itself occasionally to insure it has not been altered. This objective will sometime catch procedures that were not performed properly.

O.TOE_AVAILABLE asks the TOE designers and implementers to consider preventing as many denial of service attacks on the TOE as possible. It is desirable for the TOE to generate an alarm, even if cause is questionable, so that at the OU site the System or Security Administrator (and at an RU site the remote user) are able to effectively monitor the TOE during operation.

T.COVERT_CHANNELS - An Authorized User, System or Security Administrator may intentionally or unintentionally transmit via a covert channel, sensitive information to Unauthorized Agents who are not privileged to see it.

RATIONALE: There are times in the design of a system that the designers inadvertently or purposely design in a communication channel that allows a process to transfer information such that the system's security policy is violated. Covert Storage Channels and Covert Timing Channels are types of covert communication channels. We tried to specify reasonable protection requirements in the FTP Family of this protection profile. We call your attention, however, to the fact that covert channel analysis and protection is considered an advanced threat. Previously, covert channel analysis took place at the B2 or above assurance levels. Because this Protection Profile attempts to specify only a medium assurance level we have only included requirements which we felt reasonable at that level.

A.MISUSE_DETECT is our assumption that a misuse detection set of applications is in place and working effectively. Covert cannel events could be detected by such a mechanism.

A.USER_TRUSTED is our assumption that users are generally trustworthy and are not purposely trying to violate policy by employing covert channels.

O.CONFIDENTIALITY requires that information released by the TOE be confidentiality protected. Complying with this objective has a chance of protecting sensitive data leaving the TOE via a covert channel and limiting who has access to it.

O.PROPER_SPEC is our objective to design the system at the start so that covert channels are eliminated.

O.SECURITY_FUNCTION is an objective to limit a user's control over security mechanisms to a minimum. By so doing, we reduce the likelihood that a user will be able to exploit covert channels that might exist.

T.CRYPTANALYTIC – Unauthorized Agents may passively attack the cryptography of the TOE using cryptanalytic methods.

RATIONALE: A.CRYPTANALYTIC assumes the cryptographic methods are sufficiently strong to protect sensitive data from passive cryptanalytic attacks.

O.PROPER_SPEC requires that the TOE be properly designed to counter attacks. This means that the design implementations should be robust.

T.MALFUNCTION - Failures occur in ways that result in inappropriate access or modification of information, or inappropriate utilization of resources.

RATIONALE: This threat involves insecurities that result from malfunctions such as power supplies blowing or control boards suddenly going bad. It does not assume that anything went wrong with the system design.

A.LOGISTICS_SUPPORT allows speedy and secure recovery and service for all Authorized Users. Having an ample and protected supply of spare parts available for good maintenance and administrative personnel is a good idea in case of a malfunction. In modern computer systems the administrators, or at times the authorized users, are expected to perform first-line maintenance.

A.BACK_UP assumes the TOE can be restored to pre-malfunction status by backing up its files and configuration parameters on a regular basis. It allows service to resume from a point in which the TOE was operating normally.

O.ALARM is a necessary objective to enable System and Security Administrators at an OU site and remote users at and RU site to know as quickly as possible that the site TOE has malfunctioned. Proper alarming provides for a speedy recovery.

O.AUDIT is an objective that ensures that the TSE designers provide a robust enough audit mechanism to record TOE malfunctions.

O.BACK_UP provides for security services that must be designed into the TOE to enable either System or Security Administrators or remote users to restore TOE services to a previous secure state in the event of a malfunction.

O_{OU}.IDENTIFY_USER is an objective that ensures the designers provide that only Authorized Users will access the TOE. This applies even when the TOE has malfunctioned. The design will consider shutting down operation in the event of a malfunction rather than risk improper usage by Unauthorized Agents.

O_{RU}.IDENTIFY_USER at a RU site also insures that the authorized remote user is authenticated based on their hardware token and password

O.PROPER_SPEC is an objective that requires designers of the TOE to take proper care in adequately specifying security mechanisms that are robust enough to protect the type of data being sent through the TOE. This Protection Profile details various requirements for cryptographic operations that are suitable for sensitive information (see Class FCS: Cryptographic Support).

O.RELIABLE is the objective to counter malfunctions by designing reliability into the TOE whenever possible. The use of boards and other circuitry with built in redundancy is one technique used. Also, the developers should take care in investigating the failure rates of equipment from various manufacturers in an attempt to make the TOE reliable. Software development techniques can also be of great help in this regard (for example, Object Oriented Development).

O.SECURE_STARTUP insists that when recovering from a malfunction, the designers of the TOE were careful about re-starting and leaving the TOE in a secure state upon failure. This objective avoids saddling administrators with cumbersome start-up or recovery procedures that could lead to insecurities.

O.SELF_TEST is the objective that the TOE has been designed with the ability to check itself occasionally to insure it has not been altered. This objective will sometime catch malfunctions that were not system detected or debilitating.

O.SEPARATION can reduce the threat of a malfunction by insisting the security designers provide for the proper separation of data between and among users. Session and data separation could minimize the security impact of a malfunction.

O.TOE_AVAILABLE asks the TOE designers and implementers to consider preventing as many denial of service attacks on the TOE as possible. This would include an attacker trying to force TOE malfunctions. We would hope that security designers would alarm as many attacks of this type, even if the cause is questionable, so that the administrators are able to effectively monitor the TOE during operation.

T.MASQUERADE_BYPASS - An Unauthorized Agent may bypass identification and authorization mechanisms in order to access or modify information, or utilize system resources. Attack strategies include password guessing, password stealing, password sniffing, all followed by replay, and IP address spoofing.

RATIONALE: A.MISUSE_DETECT, by assuming that there is a Misuse Detection system in place, hopes to counter the threat somewhat. For example, it could recognize after-hours-use of a high side resource being used via a stolen password.

O.ADMIN_SECURITY_REMOTE helps prevent bypassing of identification and authentication information via the low network side because it requires the TOE to provide a secure path from a remote terminal that is doing administration. The secure path requires strong authentication.

O.ALARM requires that the System and Security Administrators at an OU site or remote users at an RU site be notified when a bypass attempt is detected. Therefore, it can possibly reduce the damage caused by the masquerader.

O.AUDIT requires that the TSE report audit events. Hopefully, some instances of identification and authentication bypass can be detected from this reporting.

O.CONFIDENTIALITY requires that a TOE provide confidentiality for the data leaving that TOE and going to another peer TOE. This can mitigate part of the threat coming from the low side because even if the identification and authentication mechanism were defeated, data seen would be encrypted.

O.CONNECT helps to mitigate the threat coming from the low side by restricting devices to which a TOE will connect to other peer TOEs so an adversary has a limited number of identities that he may masquerade as.

O.CRYPTO_SUPPORT requires the TOE to operate with cryptographic support devices that control the identity registration and privilege assignment. These devices help to prevent adversaries from identity masquerading.

O_{OU}.IDENTIFY_USER helps to counter the threat because it requires that the TOE continuously identify the user. This makes the adversary’s job harder because each packet will be authenticated.

O_{RU}.IDENTIFY_USER at a RU site also insures that the authorized remote user is authenticated based on their hardware token and password

O.INTEGRITY requires that the TOE provide integrity protection for the data leaving that TOE and going to another, peer TOE. This can mitigate part of the threat coming from the low side because even if the identification and authentication mechanism is defeated, data that might come out is integrity protected and recipient TOEs can determine if it has been changed.

O.PROPER_SPEC requires that the TOE be well designed which would include the strength of mechanisms for identification an authentication.

O.PROTECT_ADDRESSES requires the TOE to confidentiality protect the Authorized Users addresses at OU sites. This limits the knowledge the adversary has so it mitigates the threat somewhat.

O.SELF_TEST requires that the TOE test itself. This helps ensure the TOE is in proper working order so the mechanisms that thwart identity bypassing perform as desired.

T.MASQUERADE_HIJACK - An Unauthorized Agent may intrude on a properly established session in order to access or modify information, or utilize system resources.

RATIONALE: All of the rationale for the one assumption and the 11 objectives in the threat above, **T.MASQUERADE_BYPASS**, are true for this threat also.

T.MULTIPLE_PATHS - More than one path may exist for data to flow in and out of sites and may consequently bypass intended security functions.

RATIONALE: A.ADMIN is the assumption that administration is performed competently and is separated into two distinct roles, the System and Security Administrator roles. This separation is important in mitigating this threat, because two people interpreting and implementing policy can resolve problems better than one. They provide a check on one another that multiple paths have not been inserted into the environment without the awareness and consent of the Information Security Officer.

A.INFO_SECURITY_OFFICER is an assumption that a person is assigned to write and maintain site security policy and procedures that are followed by the System and Security Administrators and authorized users. This officer will state policy concerning the limitation of multiple paths through the system.

A.POLICY_COMPLIANCE helps somewhat to counter the threat assuming that the System and Security Administrators are competently perform their tasks.

There are no objectives related to the TOE to address this threat of multiple paths, however, **OE.SELF_PROTECT** is the objective that the TSE has been designed with the ability to check itself on a predictable basis to insure it has not been altered. For example, one test it would perform is system mapping. This function might catch paths added to the environment after the initial secure implementation.

T.PHYSICAL_SECURITY – Physical security of the TSE may be inadequate to either deny UA access to information which is processed or stored within the TSE, or deny the use of (or integrity of) TOE resources. Because RU sites typically are located in higher threat environments with only a single user monitoring physical security, this threat may be more significant for RU sites.

RATIONALE: The threat posed by leaving a protected enclave while travelling to a remote site with the need to perform tasks on sensitive data typically performed in a more secure site, is diverse and difficult to mitigate. A hotel room or an insecure facility is not the ideal place to perform functions, which are typically performed in a user's home enclave. From a security viewpoint remote operations in a physically less secure environment should be avoided. However, from a practical viewpoint, remote operations will never disappear and will become more commonplace in the future. The following assumptions and objectives help mitigate threats but, by no means eliminate them.

A.ADMIN establishes that there are System and Security Administrators assigned to all OU sites. These administrators are charged with helping Authorized Users implement sound security practices at both OU and RU sites.

A.BACK_UP in this threat assumes that often remote operation is short term or in an environment in which the TOE_{RU} can be returned to the OU site without too much difficulty. The OU site has professional System or Security Administrators available to help. In the case of this threat it also means that back ups performed are kept in a more security location than with the computer the remote user carries. For example, back up material may be placed on removable disks and carried with the remote user separated form the remote system and the TOE_{RU} device.

A.INFO_SECURITY_OFFICER is the assumption that a competent security professional is available to provide policy and guidance in mitigating threats to both the OU and RU site environments. The Security Officer establishes policy for remote users to follow. System and Security Administrators understand the established policy, and are eager to help Authorized Users who must travel to RU sites.

A.POLICY_COMPLIANCE is the assumption that Authorized Users will do the best job they can at following policies and procedures when located at either their OU site or when located at a more vulnerable RU site.

A.THREAT_LEVEL assumes that an UA will be sophisticated enough to take advantage of weak links. One major area of weakness is when Authorized Users leave their home base and become remote users. The assumption is that these remote users will be aware of the risk involved as they travel from the security of their protected OU site. Their awareness, training and willingness to follow sound security policy will help mitigate the threat involved.

A.TRAIN is an assumption that good security training is available to all authorized users who travel to remote sites. Such training is especially vital for AUs who travel to remote sites. This training should be tailored specifically to the environment into which the user is travelling.

O.AUDIT is the objective for the TSE to have in place a well designed and secure auditing capability. Most often this will be a capability to generate audit records and transmit them to a centralized audit manager (located within the TSE), for analysis. This capability would help prevent an AU or administrator from denying that they performed an action, and also help detect when an Unauthorized Agent has attempted unauthorized actions.

O.BACK_UP enables the RU site, AU to back up the TOE on a device that can be separated from the user's computer and that can be carried with the user or stored in a more secure environment such as a hotel safe.

O.HALT helps to mitigate the impact of the threat because it requires the TOE to stop processing and default to a secure state whenever an insecure operation or a set of insecure operations is detected. Insecure operations could be caused by an UA making errors on unfamiliar systems.

O_{OU}.IDENTIFY_USER is the objective that leads to requirements that only System and Security Administrators may access the TOE_{OU}, and that access will be performed in a proper manner. Part of proper access is strong identification of the administrator. TOE_{OU}s identify authorized users to an IP address level (and associated password) only. System and Security Administrators, and RUs are required to identify themselves with strong token-based authentication techniques.

O_{RU}.IDENTIFY_USER at a RU site also insures that the authorized remote user is authenticated based on their hardware token and password

O.TOE_USER_ASSOCIATION helps in scrutinizing interconnections through the boundary. It requires the transmitting TOE to reject connections, if the sending and receiving users are not in the TOE's list of authorized users. Therefore, an Unauthorized Agent would have to obtain all the tickets of an Authorized User in order to connect to another site.

T.POLICY_INTERPRETATION - Site Information Security Officers may not interpret organizational security policy consistently or correctly. This could result in a violation of the intended security policy when one site interprets and implements a policy differently from another site.

RATIONALE: A.ADMIN is the assumption that the OU site's administration is separated into two distinct roles, the System and Security Administrator roles. This separation is important in mitigating this threat, because two people interpreting and implementing policy can resolve problems better than one. Also, they will more likely realize when they have a differing view of policy and will be more likely to ask about these differences and resolve them. This will effectively expose interpretation problems and resolve them correctly.

A.CRYPTO_SUPPORT makes the assumption that the establishment and integrity of vital security parameters such as ACLs and keys are external to the TOE. This enables the TOE security designers to lockout inappropriate personnel from the TOE and its environment.

A.INFO_SECURITY_OFFICER is the assumption that the site has a security-proficient person who spends time and ample energy working on the site security policies and procedures, and implementation and inspection issues. This person will be cognizant of security issues that arise between sites.

A.POLICY_COMPLIANCE is the assumption that site security officers will do their best to understand and comply with established security policy. However, there is some residual risk in that no one is perfect and policy may be ambiguously written and interpreted. These assumptions and objectives will mitigate the threat of policy misinterpretation.

O.ADMIN_INTERFACE is the important objective to present security relevant event data to the administrators of the system in a manner that is user-friendly. Often, auditable data is presented in a way that does not alert the proper administrator in a way that he will understand. It is important that administrators be guided in a user-friendly manner through procedures in a manner that enhances their understanding of the security policies and procedures involved.

T.REPUDIATION - Authorized Users or Systems or Security Administrators may deny originating or receiving data transfers or performing malicious acts.

RATIONALE: A.ADMIN is the assumption that system and security administration is a split duty in the operational user site. This assumption mitigates the risk of one person only having the power to change audit and other records that record security relevant events such as who uses the system and when and what activities/modification did that person perform.

A.MISUSE.DETECT is the assumption that in the operation user site robust misuse detection is taking place that will record who did what when. Such a record could serve as proof that certain activities tied to certain people took place.

O.ADMIN_SECURITY_REMOTE is the objective to design into your architecture a trusted path between a remote administrator and his operational user site. Part of the protection such a trusted path would provide is non-repudiation between the remote device and the site.

O.AUDIT is the objective for the TOE to have in place a well designed and secure auditing capability which most often will be a capability to generate audit reports and pass them on to an audit analysis function within the TSE. This capability will help prevent a user or administrator from claiming they did not perform an action when an audit record was generated.

O.CRYPTO_SUPPORT is the objective that the cryptography designed in and implemented by the TOE has been done properly. Good, secure cryptography provides the means to reliably trust the data in audit records, for example.

O_{OU}.IDENTIFY_USER is the objective that leads to requirements that only authorized users may access the TOE and that access will be performed in a proper manner. Most TOEs identify users based on an asserted IP address and password provided upon initial connection request.

O_{RU}.IDENTIFY_USER at a RU site also insures that the authorized remote user is authenticated based on their hardware token and password

O.PROPER_SPEC is the objective to design into the TOE the proper mechanisms to securely and reliably record security relevant events. These mechanisms would help prevent claims by users and administrators that they did not perform certain actions.

T.TEMPEST Unauthorized Agents may receive sensitive data, which has radiated or is conducted from the TOE.

RATIONALE: A.TEMPEST assumes that the TOE is adequately designed to minimize the risk of sensitive data emanations. It assumes that no specific TEMPEST design or test requirements will be placed on the TOE and that good commercial design and installation practices are sufficient to address this threat.

T.TRAFFIC_ANALYSIS - Identification of Authorized Users or other sensitive information may be deduced by observing the TSE or related resources (e.g., plain text source/destination addresses, traffic volume, and human response or actions.)

RATIONALE: **O.PROPER_SPEC** is an objective that requires the designers of the system take this threat into consideration and do a competent job of designing a system that does not make traffic analysis easy for anyone.

O.PROTECT_ADDRESSES is an objective to hide the addresses of communicating entities at OU sites from easy viewing and insure the integrity of the addresses. Even casual viewing of addresses often makes event analysis easy.

T.TRANSMISSION_ERRORS - Transmission errors can cause loss of data or data integrity.

RATIONALE: This threat is both from an Agent trying to deny service and natural causes, which have the same result. It is a difficult threat to protect against and hence most of our recommendations fall in the prevention category.

A.MISUSE_DETECT assumes that the OU site has incorporated an application within its MD system that looks for transmission errors and determines, if there is a human pattern involved. If detected, alarms may be triggered and steps taken by well-trained administrators to correct the situation.

O.ALARM states that when violations occur the TOE_{OU} will be able to alarm the proper mechanisms that will perform pre-arranged alerting. Trained administrators will then be able to perform corrective action. Typically, at an RU site this alarming function will be directed to the remote user who may have only limited capability to correct the alarm condition and may require additional help from his associated home site System or Security Administrator.

O.INTEGRITY will detect whether an Agent has modified sensitive data. By performing well-established integrity functions, the TOEs will be able to check whether the original information is altered. Therefore, it will alarm appropriate personnel when transmission problems occur.

O.PROPER_SPEC can help to mitigate the threat, because it requires the TOE to be well designed and contain strong security protections that should include design features that attempt to preclude operator errors as well as excellent error checking mechanisms.

O.TOE_AVAILABLE can reduce the threat resulting in denial of service by requiring the TOE to be resistant to these types of attacks

T.UNAVAILABLE - The Internet, PSTN, or shared public network may be unavailable.

RATIONALE: This is a typical denial of service threat. In today’s environment cutting off public, shared communication channels is a common way of denying essential service to your customers. There is nothing we can specify in the way of TOE requirements that will help mitigate this threat. Therefore, we assume the threat away with **A.AVAILABLE.** **A.AVAILABLE** states, “Internet, PSTN or other required public network connections are available to the TSE when required. At best, MD and other sensing mechanisms will help detect both inadvertent and intentional attempts to deny service to system users.

P.ACCOUNT - Authorized Users, System and Security Administrators must be held accountable for security relevant actions.

RATIONALE: **A.ADMIN** assumes that there are System and Security Administrators. These are necessary because they will be relied upon to perform actions that will assist in holding Authorized Users accountable for their actions. They are also necessary because one type administrator will assist in holding the other type administrator accountable.

A.MISUSE_DETECT assumes that there is a Misuse Detection system in place. This system can provide data that will assist in holding users and administrators accountable.

O.ADMIN is necessary so that the TOE has features to allow System and Security Administrators and only them to manage it.

O.AUDIT requires the TOE to report auditable events to the Misuse Detect system. With a MD system and meaningful auditable events the organization has the capability to hold Authorized Users, administrators and UA accountable for their actions.

O.CRYPTO_SUPPORT provides for the TOE to operate with other devices that allow users to be registered, given keys, etc. These other mechanisms contribute to providing accountability.

O_{OU}.IDENTIFY_USER requires the TOE_{OU} to continuously identify users. This ties users to actions, so they can be held accountable.

O_{RU}.IDENTIFY_USER at a RU site also insures that the authorized remote user is authenticated based on their hardware token and password

O.PROPER_SPEC requires that the mechanisms that affect accountability be designed well.

P.ADMIN_SECURITY_RESTRICTED - Only Authorized System and Security Administrators and trained maintainers may administer or repair security mechanisms in their assigned site TSE. At RU sites, limited on-site administration will be performed by the RU, but only as authorized and directed by their associated home OU site, System and Security Administrator.

RATIONALE: **A.MISUSE_DETECT** assumes misuse detection is in place at both the OU and sites that may detect evidence of unauthorized administration.

O.ADMIN requires that the TOE provide functions that ensure that only System and Security Administrators and remote, Authorized Users can access administrative functionality.

O.ADMIN_SECURITY_REMOTE requires the TOE to provide a secure path capability to a RU site. This path includes authentication that would be used to identify remote, Authorized Users so that their administrative functionality can be limited according to site security policy.

O.ALARM can help minimize the impact of a person improperly administering or repairing security mechanisms within the TSE. The objective of having an alarm function is to alert the proper personnel as quickly as possible that someone has performed or is trying to perform a security relevant event of this type.

O.AUDIT can help to implement the policy but only by deterrence. It requires that auditing be done which could help to catch improper administering.

O.CRYPTO_SUPPORT requires the TOE to interface with crypto support devices that would include certificate and privilege issuing authorities. This would be used to distinguish administrators, including remote, Authorized Uses, from other users.

O_{OU}.IDENTIFY_USER and **O_{RU}.IDENTIFY_USER** require the TOE to identify users, which includes administrators and remote users. This is a necessary step in controlling who can administer the TOE.

O.PROPER_SPEC requires the TOE to be well designed which helps proper implementation of this policy

P.AUDIT_REVIEW - Audit data will be reviewed, analyzed, and as appropriate, acted upon.

RATIONALE: A.INFO_SECURITY_OFFICER is the assumption that the site has a security-proficient security officer who spends time and ample energy working on the site security policies and procedures, and implementation and inspection issues. This person will be cognizant of security issues that arise and realize the importance of performing timely audit review.

A.POLICY_COMPLIANCE is the assumption that site security personnel will do their best to understand and comply with established security policy. However, there is some residual risk in that no one is perfect and policy may be ambiguously written and interpreted. Also, time factors effecting administrators could occur in that they are addressing other issues they deem more important and they never find time to perform the audit review. The assumptions and objective we list will mitigate this risk.

O.AUDIT insists that there exists at OU sites a robust enough auditing package that is user friendly and relieves security personnel of much of the boring work of audit analysis and review. Also, it provides that the auditing be performed at RU sites for off-loading into the audit software within the MD system.

P.AVAILABLE - Access to communications such as the Internet, PSTN or other public network connections will be available to the AU when required. An Information Security Officer will develop policy

governing the use of these communications and the System and Security Administrators will implement this policy.

RATIONALE: A.ADMIN establishes that there are System and Security Administrators, who are normally trusted. These administrators are charged with the responsibility of implementing communications availability policy within their organization.

A.AVAILABLE assumes that the communications infrastructure your organization needs are available, so that this policy is feasible most of the time.

A.INFO_SECURITY_OFFICER is an assumption that a competent security professional is assigned to write and maintain site security policy and procedures that are followed by the System and Security Administrators and Authorized Users. One such policy is the statement of who an Authorized User is and the care regarding how that judgement is implemented by the administrators.

A.MISUSE_DETECT helps implement this policy, because it specifies that misuse detection mechanisms are in place, some of which are checking that external communications are available.

A.LOGISTICS_SUPPORT helps in that, if an Agent is successful in an attack that actually causes physical harm to the TOE or TSE, by having a supply of spares that your Administrators or remote Authorized Users can apply mitigates the risk of denial of service.

O.ADMIN_INTERFACE is the important objective to present security relevant data to the administrators of the system in a manner that is user-friendly. It is important that administrators be able to easily spot when communications are unavailable and be guided through corrective actions in a straightforward manner.

O.ALARM helps implement this policy by requiring the TOE to detect when communications are unavailable and notify the System and Security Administrators as well as remote Authorized Users.

O_{OU}.IDENTIFY_USER and **O_{RU}.IDENTIFY_USER** are important so that user identification is checked during the TOE operation and an alarm triggered, if this check fails. This check is important to ensure that uses of communications channels are appropriate.

P.COMPLY - The implementation and use of the organization's IT systems must comply with all applicable laws, regulations, and contractual agreements imposed on the organization.

RATIONALE: **A.INFO_SECURITY_OFFICER** is an assumption that there is an information security officer at each site whose job is to oversee policy compliance.

A.MISUSE_DETECT assumes that there is a Misuse Detection system within the TSE. The TOE will generate audit records and report them to the MD system. This analysis capability helps to encourage the users to comply with applicable laws, policies and procedures. .

A.POLICY_COMPLIANCE assumes that the users and administrators will do their best to obey the policies. However, we know that this assumption is not satisfactory by itself.

A_{OU}.PHYSICAL_SECURITY assumes that physical protections are provided to protect the sensitive information in accordance with all due care. It assumes there is a physical boundary around the TSE at the OU site and adequate protection provided for equipment and data therein. This boundary definition aids in defining the electrical communications boundary.

At a RU site, **A_{RU}.PHYSICAL_SECURITY** assumes that physical security is typically less robust than at an OU site. Consequently, there is additional burden placed on procedural controls and perhaps other mechanisms included within the TSE which will insure that stored data is secured by techniques such as physical secure storage of media or encryption when left unattended by the RU site AU. These additional objectives are captured in OE_{RU}.PHYSICAL_SECURITY.

O.CONFIDENTIALITY is required so that sensitive information can be protected in accordance with the laws, policy and procedures when it is released over a network connecting users without the proper authorizations.

O.INTEGRITY is required so that sensitive information can be protected from modification in accordance with the laws, policy and procedures when it is released over a network connecting users without the proper authorizations.

P.DEFEND The TOE shall defend itself from improper operation or malfunction caused by attacks via the communications channels.

RATIONALE: A.ADMIN establishes that there are System and Security Administrators, who are normally trusted. These administrators are charged with the responsibility of implementing the policy of defending the IT environment from attack.

A.AVAILABLE assumes that the communications infrastructure your organization needs is available, so that administrators can implement defend policy effectively.

A.INFO_SECURITY_OFFICER is an assumption that a competent security professional is assigned to write and maintain site security policy and procedures that are followed by the System and Security Administrators.   One such policy is the statement of what defending the IT environment means and limitations, if any, on defending it.

A.MISUSE_DETECT helps implement this policy, because it says that in the TSE misuse detection mechanisms are in place, some of which are checking for inappropriate access and other system misuse. The TOE generates audit reports and provides them to the MD system for analysis.

A.TRAIN is the assumption that administrators of the TSE are properly trained to defend the IT environment. This means that users and administrators come to the organization trained in this skill, or that the organization has the means to train these people, or some combination of the two.

O.ALARM helps implement this policy by requiring the TOE to detect various security violations and to notify the System and Security Administrators as well as remote Authorized Users, when they occur.

O.CRYPTO_SUPPORT helps in that it is vital that the cryptographic support mechanisms that the TOE uses be designed to work with the TOE securely.   Attacks will often test these interfaces for security weaknesses.

O.HALT is an important objective in that when the TOE is signaled or in other ways senses that it is under attack, it should shut down its operation and alert the System and Security administrators or remote Authorized User to take appropriate action.

O_{OU}.IDENTIFY_USER is important so that user identification is continuously checked during the TOE operation and an alarm triggered, if this check fails. This check is initially based on asserted IP address and provided password. Continuous authentication is based on only the asserted IP address contained in each packet.

O_{RU}.IDENTIFY_USER at a RU site also insures that the authorized remote user is authenticated based on their hardware token and password.

O.PROPER_SPEC provides some assurance that the designers thoroughly discussed attack scenarios and designed the TOE to be immune to them.

O.SECURITY_FUNCTION provides some assurance that the minimal set of personnel has access to TOE security functions.

O.SELF_TEST gives us the assurance that the TOE has viable self tests running that enable it to protect itself. Typically, the TOE does this by ensuring it is running code that is consistent.

O.TOE_AVAILABLE states that the designers will attempt to use techniques that make the TOE resilient to denial-of-service attacks.

O.TOE_USER_ASSOCIATION helps implement this policy by assuring that Authorized Users are not Unauthorized Agents.

P.DISTRIBUTION - Control of the issuing of security relevant TOE hardware, software and all other resources will be maintained.

RATIONALE: **A.INFO_SECURITY_OFFICER** is the assumption that the site has a security-proficient person who spends time and ample energy working on the site security policies and procedures, and implementation and inspection issues. This person will be cognizant of security issues that arise and realize the importance of strictly controlling TOE hardware and software.

A.POLICY_COMPLIANCE assumes administrators will do their best to obey organizational securities policies. Controlling security relevant hardware and software is an important function. However, we know that often administrators are side-tracked with time sensitive, urgent issues such as downtime and access control problems. They may not perform this function in accordance with strict organizational policy. The assumptions and objectives in this section will help ensure this policy is implemented properly.

O.ADMIN is necessary so that the TSE has features, such as secure databases to allow System and Security Administrators and only them to manage the TOE software, hardware and associated devices. Remote Authorized Users will normally not manage TOE hardware or software.

O.ADMIN_INTERFACE is the important objective to present security relevant data to the administrators of the system in a manner that is user-friendly. It is important that administrators be guided in a user-friendly manner through procedures in a manner that enhances their understanding of the security policies and procedures involved.

P.DUE_CARE -The organization's IT systems must be implemented, maintained and operated in a manner that represents due care and diligence with respect to risks to the organization. The level of security afforded the IT system must be in accordance with what is considered prudent by the organization's or system's accrediting authority.

RATIONALE: The whole process in generating this protection profile has attempted to consider what would be prudent requirements for operating an IT system intended to process and protect sensitive information. Therefore, all the assumptions except **A.AVAILABLE** are relevant to, and all the objectives are driven by, this due care policy. They will not be individually rationalized here, but are listed in Table 4.

P.LABEL - All unclassified sensitive or COI information will be appropriately identified regardless of physical or electronic representation.

RATIONALE: A.INFO_SECURITY_OFFICER is the assumption that the site has a security-proficient person(s) who spends time and ample energy working on the organization's security policies and procedures, and implementation and inspection issues. This person(s) is cognizant of security issues and realizes the importance of properly labeling information. It also assumed this person helps train personnel attached to the site the importance of labeling information properly.

A.POLICY_COMPLIANCE assumes that personnel will willingly and competently comply with all organizational policies. It does acknowledge that there are times that this assumption about the attitudes of personnel is not warranted.   Thus, risk exists.

P.MANAGE - The TOEs shall be managed and maintained such that their security functions are implemented and preserved throughout their operational lifetime.

RATIONALE: A.ADMIN assumes that there are Security and System Administrators that manage the TOEs throughout their installed lifetime.

A.INFO_SECURITY_OFFICER assumes that there is an Information Security Officer that writes the policy on how the TOEs are to be managed.

A.POLICY_COMPLIANCE assumes that the administrators and remote Authorized Users will carry out organizational security policy.

O.ADMIN is necessary to provide a requirement for TOEs to have functions that allow administrators to manage them.

O.ADMIN_INTERFACE is necessary to provide a requirement for TOEs to have a friendly interface in order to aid in minimizing errors that Security Administrators might make.

O.ADMIN_SECURITY_REMOTE provides for TOEs to be administered remotely.

O.AUDIT is required because auditing is an essential tool in managing an organization securely.

O.SELF_TEST is required, because it is an essential tool in managing an organization securely.

P.PERSONNEL_TRUST_COI - All Authorized Users, System and Security Administrators and maintainers of TOE resources, which process COI information or Authorized Users of COI information will be, granted privileges for their specific COI privilege level.

RATIONALE: In order for an organization to succeed, it must hire System and Security Administrators and Authorized Users whom it can trust with resources and capabilities that will enhance their ability to accomplish their mission. This work must be accomplished securely to protect both the organization and its workers/users. The Administrators' role is an especially critical one and, hence, the organization must take positive steps to ensure they meet minimum standards of trust prior to hiring. The same is true for Authorized Users. An AU who violates the trust given him can cause harm to any organization. The most significant harm, however, is caused by corrupt administrators. There are various ways an organization can help itself trust administrators and Authorized Users. We have discussed several in this Protection Profile.

A.USER_TRUSTED helps to affect this policy by assuming that Authorized Users are trusted, mainly because adequate checks on their pasts have been made before hiring them. However, it also recognizes that users sometime cannot be trusted, leaving the policy risky, but still necessary.

O.CRYPTO_SUPPORT is important in insuring the establishment and integrity of vital security parameters such as ACLs and keys so that inappropriate personnel are locked out from using the TOE and its environment. If privileges are to be given, they must be given to a limited set of people and their communications protected and delivered accurately.

P.PERSONNEL_TRUST_MINIMUM - All Authorized Users, System and Security Administrators and maintainers of TOE resources will possess a minimum sensitive privilege level.

RATIONALE: In order for an organization to succeed, it must hire System and Security Administrators who it can trust with resources and capabilities that will enhance an employee's ability to manage their environment. The bottom line must be to make it easy for real users to do real work, yet do it securely to protect all concerned. The Administrators' role is a key one and, hence, the organization must take positive steps to ensure they meet minimum standards of trust. There are various ways an organization can help itself trust Administrators and Authorized Users. We have discussed several in this Protection Profile.

A.USER_TRUSTED helps to effect this policy by assuming that Authorized Users are trusted, mainly because adequate checks on their past have been made before hiring them. However, it also recognizes that users sometime cannot be trusted, leaving the policy risky, but necessary.

O.CRYPTO_SUPPORT is important in insuring the establishment and integrity of vital security parameters such as ACLs and keys so that inappropriate personnel are locked out from using the TOE and its environment. If privileges are to be given, they must be given to a limited set of people and their communications protected and delivered accurately.

P. PROCEDURES - Procedures will be in place to restrict inadvertent disclosure or modification of sensitive information or improper utilization of resources in the TSE. Examples: Printed material handling procedures, procedures to lock computers when unattended, and guidelines for proper disposal of media.

RATIONALE: A.INFO _SECURITY_OFFICER is the assumption that the site has a security-proficient professional who spends time and ample energy working on the site security policies and procedures, and implementation and inspection issues. This person(s) is cognizant of security issues and realizes the importance of establishing well thought out, written procedures that site personnel understand and respect. This security professional helps train personnel on the importance of following procedures and where they can easily find them.

A.POLICY_COMPLIANCE assumes that personnel will willingly and competently comply with site policies. It does acknowledge that there are times that this assumption about the attitudes of personnel is not warranted. Thus, risk exists.

O.ADMIN_INTERFACE is the objective to present security relevant data to the administrators of the system in a manner that is user-friendly. It is important that administrators be guided in a user-friendly manner through procedures in a manner that enhances their understanding of the security policies and procedures involved.

O.TOE_AVAILABLE is the objective that the TOE will be resilient to denial of service attacks. The TOE must be available so that one site can interact securely with another site or an individual. This is important to achieve consistent interpretation and availability of policies throughout the organization.

P.PROTECT - Confidentiality and integrity protection must be applied to sensitive information before it leaves the TSE to a network with less privileged users.

RATIONALE: A.ADMIN establishes that there are System and Security Administrators, who are normally trusted. These administrators are charged with the responsibility of ensuring that mechanisms are always in place that implements this information protect policy.

A.CRYPTO_SUPPORT is an assumption that the security mechanisms necessary to implement this policy are available and provided.

A.INFO_SECURITY_OFFICER is an assumption that at least one competent security professional is assigned to write and maintain site security policy and procedures that are followed by the System and Security Administrators and all Authorized Users.

A.MISUSE_DETECT helps to mitigate the threat because it says that misuse detection mechanisms are in place, some of which are checking for inappropriate TOE operations.

A.TRAIN is the assumption that all users and administrators of the TSE are properly trained. This means that users and administrators come to the organization trained in how to ensure mechanisms are in place to perform confidentiality and integrity protection, or that the organization has the means to train these people in this skill, or some combination of the two.

O.ALARM helps implement this policy by requiring the TOE to detect violations to this policy and to notify the System and Security Administrators or the remote Authorized Users, when problems occur.

O.CONFIDENTIALITY is an objective that focuses on a primary aspect of this policy.

O.CRYPTO_SUPPORT helps in that it is vital that the cryptographic support mechanisms that the TOE uses are available and designed to work with the TOE securely.

O.HALT specifies that when the TOE is signaled or in other ways senses that confidentiality or integrity mechanisms are not working properly, it will shut down its operation and alert the security administrator or the remote Authorized User to take appropriate action.

O.INTEGRITY is an objective that focuses on a primary aspect of this policy.

O.PROTECT_ADDRESSES states that we wish the identification and addresses of authorized users at OU sites to be integrity and confidentiality protected.

O.SECURITY_FUNCTION provides some assurance that the minimal set of personnel has access to TOE security functions.

O.SELF_TEST gives us the assurance that the TOE has viable self tests running that enable it to detect when this policy is not being followed. Typically, the TOE does this by ensuring it is running fixed, controlled code.

P.RECIPIENTS - Communications through the TOE shall be only between and among Authorized Users or System and Security Administrators.

RATIONALE: A.ADMIN establishes that there are System and Security Administrators, who are normally trusted. These administrators can help to avert compromise or damage caused by intentional or accidental access list violations that permit Agents to view and manipulate material that they are not authorized to access.

A.INFO_SECURITY_OFFICER is an assumption that a competent security professional is assigned to write and maintain site security policy and procedures that are followed by the System and Security Administrators. One such policy is the statement of who an authorized user is and the care regarding how that judgement is implemented by the administrators.

A.MISUSE_DETECT helps to implement this policy, because it says that misuse detection mechanisms are in place, some of which are checking for inappropriate access and other system misuse.

A.POLICY_COMPLIANCE also helps with this policy by assuming that Authorized Users and System and Security Administrators are competent and will accurately carry out the security policy both at OU and RU sites. The implication is they will typically not make mistakes. However, there remains residual risk because the assumption is not 100% achievable. The residual risk is mitigated somewhat by having split administrative duties.

O.ADMIN helps implement this policy by requiring the TOE to have its security functions managed and accessed only by System and Security Administrators and authorized remote users

O.AUDIT requires the TOE to perform auditing so that people can be held accountable for their actions. This provides some deterrence, which aids in implementing this policy.

O.ADMIN_INTERFACE helps with this policy by requiring the TOE to have a user-friendly interface for the administrators and remote Authorized Users so that errors in managing access list and IP addresses are minimized.

O.ALARM helps with this policy by requiring the TOE to detect violations of use of the TOE and to notify the System and Security Administrators or remote Authorized Users when possible.

O.CONNECT helps in implementing this policy by requiring that, if an individual comes from a side of the network that has personnel with unknown levels of trust, there are specific restrictions regarding the devices to which a TOE can connect. Therefore, an adversary has a limited number of identities that he may assume.

O.HALT helps implement this policy, because it requires the TOE to stop processing and default to a secure state whenever an insecure operation is detected.

O_{OU}.IDENTIFY_USER is important so that user identification is continuously checked during the TOE_{OU} operation and an alarm triggered, if this check fails. This check is initially based on a user provided password and asserted IP address. Continuous authenticated is based on only the asserted IP address contained in each data packet.

O_{RU}.IDENTIFY_USER at a RU site also insures that the authorized remote user is authenticated based on their hardware token and password.

O.PROTECT_ADDRESSES is also vital in that the attacker not be allowed to substitute additional or replacement addresses or destroy addresses of communications originating from OU sites.

O.TOE_USER_ASSOCIATION helps in scrutinizing interconnections through the boundary. It requires the transmitting TOE to reject connections, if the sending and receiving users are not in the TOE's list of authorized users.

P.RELEASE_NON-SENSITIVE - All non-sensitive information in a sensitive or COI environment is implicitly marked Sensitive or COI respectively.

Information in these environments must be reviewed or filtered before releasing it unprotected outside the TSE.

RATIONALE: This policy means that all non-sensitive information in an enclave will be considered Sensitive system-high or COI, whether marked or not, and reviewed before it is released unprotected outside the enclave. The TOE is not intended to have a bypass capability that would allow information to go from one sensitivity level to a lessor level without confidentiality and integrity protection applied. Therefore, no unprotected data payload information would leave the TOE. If the rest of the system outside the TOE has a bypass capability, it should be well designed, because that situation represents significant risk.

A.INFO_SECURITY_OFFICER is a related assumption because it is the Information Security Officer who would write the policy concerning implicit sensitivity marking.

A.POLICY_COMPLIANCE assumes that users and administrators in the enclave will do their best to obey the policies of OU or RU site. Of course residual risk still exists, because there are humans and imperfect hardware and software involved.

O.CONFIDENTIALITY prohibits the TOE from having a plain text bypass capability. Therefore, all data payload information leaving an OU or RU TOE would be encrypted.

O.INTEGRITY prohibits both the OU and RU TOE from having a bypass capability that would avoid applying data integrity protection.

P.REMOTE_SECURITY_ADMIN - Authorized System and Security Administrators may remotely administer devices in the TSE through protected external communication channels.

RATIONALE: O.ADMIN requires that TOE's contain functions that ensure only System and Security Administrators can access administrative functionality.

O.ADMIN_SECURITY_REMOTE requires TOE$_{OU}$s to provide a secure path capability to TOE$_{RU}$.

O.CRYPTO_SUPPORT requires TOEs to interface with crypto support devices that would include certificate and privilege issuing authorities. This capability is necessary to distinguish administrators from other Authorized Users.

O$_{OU}$.IDENTIFY_USER requires TOE$_{OU}$s to identify Authorized Users, and System and Security Administrators, a necessary step in controlling who can administer a TOE$_{OU}$.

O$_{RU}$.IDENTIFY_USER at a RU site also insures that the authorized remote user is authenticated based on their hardware token and password.

O.PROPER_SPEC requires both the TOE_{OU} and the TOE_{RU} to be well designed which helps with this policy.

P.TOE_USAGE - TOE, usage, and the ability to release data from a TOE, will be limited to personnel who have been properly authenticated and deemed to be Authorized Users, System or Security Administrators. Remote User (RU) privileges, and usage of a TOE from a remote location, will be tightly controlled and procedurally limited to situations where there is a strong operational requirement.

RATIONALE: We assume that not all personnel in a sensitive enclave should have the privilege of communicating sensitive information outside the enclave. Therefore, a selection process is necessary to limit the use of the TOE. Likewise, the use of remote devices in the hands of personnel who often are not as computer literate as you'd like presents a security risk to the Operational User Site. Yet, operational necessity dictates that this risk is taken as essential mission personnel are travel. One step that an Information Security Officer and Security Administrator can take to mitigate this risk is to ensure that both formal and informal "training" and awareness sessions are provided to travelling, remote users. When these users are aware of the risks to the site via a remote device and are well trained in the whys and hows of reducing the threat, security improves.

A.INFO_SECURITY_OFFICER is a related assumption, because it is the Information Security Officer who would write the policy about TOE usage. This assumption is that he does his job well and implements policy appropriately.

A.MISUSE_DETECT is the assumption that in the OU site's robust, misuse detection is taking place that might detect improper TOE_{OU} and TOE_{RU} usage.

A.POLICY_COMPLIANCE is the assumption that personnel will willingly and competently comply with site policies regarding the proper utilization of TOE resources. It does acknowledge that there are times that this assumption about the actions of personnel is not warranted. However, we assume that training and other means to keep travelling personnel aware is not wasted time.

A.USER_TRUSTED helps to affect this policy by assuming that Authorized Users are trusted, mainly because adequate checks on their pasts have been made before hiring them. However, it also recognizes that users sometime cannot be trusted, leaving the policy risky, but still necessary.

O.ADMIN_INTERFACE is the objective to present security relevant data to the administrators of the system in a manner that is user-friendly. It is important that administrators be guided in a user-friendly manner through security procedures such as those required by this policy in a manner that enhances their understanding of both the security policies and procedures involved.

O.CONNECT helps in that it requires proper identification between Authorized Users prior to the TOEs connecting and communicating.

O_{OU}.IDENTIFY_USER is an objective that requires the TOE_{OU} to help perform the scrutiny of data flow through the boundary. It requires users to be identified within their protected environment by at least their IP address and provided password. Peer TOEs to peer TOEs are authenticated to each other by issued X.509 certificates and authentication identity mechanisms. Adherence to this objective will be very useful in limiting the use of the TOE_{OU} by only authorized personnel.

O_{RU}.IDENTIFY_USER at a RU site also insures that the authorized remote user is authenticated based on their hardware token and password.

O.PROPER_SPEC requires the TOE to be well designed which helps ensure the mechanisms to implement this policy properly are in place and effectively used.

O.SECURITY_FUNCTION is an objective to limit Authorized User's control over security mechanisms to a minimum. By so doing, we reduce the likelihood that an agent will be able to use the TOE.

O.TOE_USER_ASSOCIATION helps in scrutinizing interconnections through the boundary. It requires the transmitting TOE to reject connections if the sending and receiving users are not in the TOE's list of authorized users.

P.TRAIN - All Authorized Users, Systems and Security Administrators and maintainers of TOE resources will be properly trained to the level of their responsibility.

RATIONALE: A.TRAIN is the assumption that all users and administrators of the TSE are properly trained. This means that Authorized Users and administrators come to the organization trained, or that the organization has the means to train these people, or some combination of the two.

P.TSE_CONNECTIONS - All connections between the TSE and external networks will be controlled. At an OU site these connections will be made through boundary protection functions which are physically isolated and accessible by only the System or Security Administrators. At a remote site, connections between the TSE and the network will be established by the RU and boundary protection functionality will be under the direction and procedural control of the RU.

RATIONALE: A.ADMIN assumes that there are administrators who attempt to carry out site policies that include prohibiting unauthorized connections.

A.MISUSE_DETECT is related to the policy, because it could possibly sense communications that did not come through the defined boundary interconnection(s).

A.POLICY_COMPLIANCE assumes that personnel will make only authorized connections.

A_{OU}.PHYSICAL_SECURITY assumes there is a physical boundary around the TSE at the OU site and protection provided to what's inside. This boundary definition aids in defining the electrical communications boundary.

At a RU site, **A_{RU}.PHYSICAL_SECURITY** assumes that physical security is typically less robust than at an OU site. Consequently, there is additional burden placed on procedural controls and perhaps other mechanisms included within the TSE which will insure that stored data is secured by techniques such as physical secure storage of media or encryption when left unattended by the RU site AU. These additional objectives are captured in OE_{RU}.PHYSICAL_SECURITY.

O_{OU}.IDENTIFY_USER is an objective that requires the TOE_{OU} to help perform the scrutiny of data flow through the boundary. It requires Authorized Users to be by at least their IP address and user provided password. Peer TOEs to peer TOEs are authenticated to each other by issued X.509 certificates and authentication identity mechanisms. Adherence to this objective will be very useful in limiting the use of the TOE by only authorized personnel.

O_{RU}.IDENTIFY_USER at a RU site also insures that the authorized remote user is authenticated based on their hardware token and password.

O.TOE_USER_ASSOCIATION helps in scrutinizing interconnections through the boundary. It requires the transmitting TOE to reject connections if the sending and receiving users are not in the TOE's list of authorized users.

P.USAGE The organization's IT resources must be used only for authorized purposes.

RATIONALE: A.INFO_SECURITY_OFFICER is a related assumption, because it is he who would write system utilization policy. This assumption is that this person does his job well and implements policy that helps the organization identify authorized TOE utilization.

A.POLICY_COMPLIANCE assumes that personnel will willingly and competently comply with OU and RU site policies regarding the proper utilization of TOE resources. It acknowledges that there are times that this assumption about the action of personnel is not warranted.

O_{OU}.IDENTIFY_USER is an objective that requires the TOE to help perform the scrutiny of data flow through its boundary protection. It requires Authorized Users to be identified within their OU site by at least their IP address and user provided password. Peer TOEs to peer TOEs are authenticated to each other by issued X.509 certificates and authentication identity mechanisms. Adherence to this objective will be very useful in limiting the use of the TOE by only authorized personnel.

O_{RU}.IDENTIFY_USER at a RU site also insures that the authorized remote user is authenticated based on their hardware token and password.

O.PROPER_SPEC helps to enforce this policy, because it requires the TOE to be well designed, and contain strong security protections such as **O_{OU}.IDENTIFY_USER** and **O.TOE_USER_ASSOCIATION**.

O.TOE_USER_ASSOCIATION helps in scrutinizing interconnections through the boundary. It requires the transmitting TOE to reject connections, if the sending and receiving users are not in the TOE's list of authorized users.

6.2 Security Objectives Coverage

This section contains a mapping table and individual arguments for each Objective covered. Table 6 lists either the TOE or environmental Objective that requires coverage in the first column. The second column provides a cross-index of Policies and/or Threats that are addressed, in part or in full, for each Objective. TOE components and/or environmental requirements that cover each Objective are listed in the third column. Following this table are individual arguments for the coverage of each Objective.

Table 6 Security Objective Mapping to Functional Security Requirements

TOE_{OU} Objectives	Threats / Policies	Requirements

O.ADMIN	T.ATTACK_DATA;
	T.BAD_ACCESS_INAPPROPRIATE;
	T.BAD_ACCESS_UNAUTHORISED;
	T.BAD_DESIGN_COMPLEXITY;
	P.ACCOUNT;
	P.ADMIN_SECURITY_RESTRICTED;
	P.DISTRIBUTION;
	P.DUE_CARE;
	P.MANAGE;
	P.RECIPIENTS;
	P.REMOTE_SECURITY_ADMIN
		FAU_ARP
		FAU_GEN
		FAU_SAR
		FMT_SMR
		FAU_SEL
		FTA_TSE
		FIA_ATD
		FPR_UNO
		FIA_UID
		FIA_UAU
		FIA_AFL
		FMT_MOF
		FMT_MTD
		FMT_MSA
		FPT_STM
		FPT_TDC
		FAU_SAA
		FDP_IFC

TOE_{OU} Objectives	Threats / Policies	Requirements

O.ADMIN_INTERFACE	T.BAD_ADMIN_ERROR;
	T.BAD_DESIGN_COMPLEXITY;
	T.BAD_PROCEDURES;
	T.POLICY_INTERPRETATION;
	P.AVAILABLE;
	P.DISTRIBUTION;
	P.DUE_CARE;
	P.MANAGE;
	P.PROCEDURES;
	P.RECIPIENTS;
	P.TOE_USAGE
		FAU_SAR
		FMT_SMR
		FAU_SEL

O.ADMIN_SECURITY_REMOTE	T.BAD_ACCESS_UNAUTHORISED;
	T.BAD_AUDIT_UNTRACEABLE;
	T.MASQUERADE_BYPASS;
	T.MASQUERADE_HIJACK;
	T.REPUDIATION;
	P.ADMIN_SECURITY_RESTRICTED;
	P.DUE_CARE;
	P.MANAGE;
	P.REMOTE_SECURITY_ADMIN
		FAU_ARP
		FAU_GEN
		FAU_SAR
		FMT_SMR
		FAU_SEL
		FTA_TSE
		FIA_ATD
		FPR_UNO
		FIA_UID
		FIA_UAU
		FIA_AFL
		FMT_MOF
		FMT_MTD
		FMT_MSA
		FPT_STM
		FTP_ITC
		FIA_SOS
		FCS_CKM
		FCS_COP
		FDP_ACF
		FPT_TDC
		FAU_SAA
		FDP_IFC

O.ADMIN_SEPARATE	T.ATTACK_DATA	FIA_ATD FIA_UAU FIA_USB FMT_SMR FMT_MTD FMT_MOF FMT_MSA FAU_SAR FAU_SEL FDP_IFC FDP_IFF

O.ALARM	T.ATTACK_DATA;
	T.BAD_ACCESS_INAPPROPRIATE;
	T.BAD_ACCESS_UNAUTHORISED;
	T.BAD_ADMIN_ERROR;
	T.BAD_AUDIT_OVERFLOW;
	T.BAD_AUDIT_UNDETECTED;
	T.BAD_AUDIT_UNTRACEABLE;
	T.BAD_DESIGN_EXTERNAL;
	T.BAD_PROCEDURES;
		FAU_ARP
		FAU_GEN
		FPT_PHP
		FRU_FLT
		FAU_SAA

TOE_{OU} Objectives	**Threats / Policies**	**Requirements**

	T.MALFUNCTION;
	T.MASQUERADE_BYPASS;
	T.MASQUERADE_HIJACK
	T.TRANSMISSION_ERRORS;
	P.ADMIN_SECURITY_RESTRICTED;
	P.DEFEND;
	P.DUE_CARE;
	P.PROTECT;
	P.RECIPIENTS	

O.AUDIT	T.BAD_ACCESS_INAPPROPRIATE;
	T.BAD_ACCESS_UNAUTHORISED;
	T.BAD_ADMIN_ERROR;
	T.BAD_AUDIT_OVERFLOW;
	T.BAD_AUDIT_SEQUENCE;
	T.BAD_AUDIT_UNDETECTED;
	T.BAD_AUDIT_UNTRACEABLE;
	T.MALFUNCTION;
	T.MASQUERADE_BYPASS;
	T.MASQURADE_HIJACK;
	T.PHYSICAL_SECURITY;
	T.REPUDIATION;
	P.ACCOUNT;
	P.ADMIN_SECURITY_RESTRICTED;
	P.AUDIT_REVIEW;
	P.DUE_CARE;
	P.MANAGE;
	P.RECIPIENTS
		FMT_MTD
		FMT_MOF
		FMT_MSA
		FIA_UID
		FIA_UAU
		
		FPT_ITI
		FAU_GEN
		FAU_ARP
		FAU_SEL
		FIA_AFL
		FPT_STM
		FPT_TDC
		FAU_SAA
		FDP_IFC
		FDP_IFC

O.BACK_UP	T.ATTACK_DATA;
	T.BAD_ACCESS_INAPPROPRIATE;
	T.BAD_ACCESS_UNAUTHORISED;
	T.BAD_ADMIN_ERROR;
	T.BAD_DESIGN_COMPLEXITY;
	T.BAD_DESGN_EXTERNAL
	T.BAD_DESIGN_SECURITY_FUNCTION_
	CORRUPTION;
	T.BAD_PROCEDURES;
	T.MALFUNCTION;
	P.DUE_CARE
		FRU_FLT
		FAU_GEN

O.CONFIDENTIALITY	T.BAD_ACCESS_UNAUTHORISED;
	T.COVERT_CHANNELS;
	T.MASQUERADE_BYPASS;
	T.MASQUERADE_HIJACK;
	P.COMPLY;
	P.DUE_CARE
	P.PROTECT
	P.RELEASE_NON-SENSITIVE
		FCS_CKM
		FDP_ACC
		FDP_ACF
		FDP_ETC
		FDP_ITC
		FDP_RIP
		FCS_COP

O.CONNECT	T.BAD_ACCESS_UNAUTHORISED;
	T.MASQUERADE_BYPASS;
	T.MASQUERADE_HIJACK;
	P.DUE_CARE;
	P.RECIPENTS;
	P.TOE_USAGE
		FIA_ATD
		FIA_SOS
		
		FIA_UID
		FIA_UAU
		FCS_CKM
		FCS_COP
		FDP_ACC

TOE$_{OU}$ Objectives	Threats / Policies	Requirements
		FDP_ACF FDP_ITC

O.CRYPTO_SUPPORT	T.BAD_ACCESS_UNAUTHORISED;
	T.MASQUERADE_BYPASS;
	T.MASQUERADE_HIJACK;
	T.REPUDIATION;
	P.ACCOUNT;
	P.ADMIN_SECURITY_RESTRICTED;
	P.DEFEND;
	P.DUE_CARE;
	P.PERSONNEL_TRUST_COI;
	P.PERSONNEL_TRUSTED_MINIMUM
	P.PROTECT;
	P.REMOTE_SECURITY_ADMIN
		FTP_ITC
		FIA_ATD
		FIA_SOS
		FMT_MTD
		FPT_STM
		FPT_TDC
		FTP_ITI

O.HALT	T.ATTACK_DATA;
	T.BAD_ADMIN_ERROR
	T.PHYSICAL_SECURITY;
	P.DEFEND;
	P.DUE_CARE;
	P.PROTECT
	P.RECIPIENTS
		FPT_FLT
		FAU_GEN
		FPT_RCV
		FPT_FLS
		FAU_ARP
		FAU_SAA

O.INTEGRITY	T.ATTACK_DATA;
	T.BAD_ACCESS_UNAUTHORISED;
	T.MASQUERADE_BYPASS;
	T.MASQUERADE_HIJACK;
	T.TRANSMISSION_ERRORS;
	P.COMPLY;
	P.DUE_CARE;
	P.PROTECT;
	P.REFERENCE_NON-SENSITIVE
		FDP_ETC
		FPT_ITI
		FPT_STM
		FDP_ITC

O.PROPER_SPEC	T.ATTACK_DATA;
	T.BAD_ACCESS_INAPPROPRIATE;
	T.BAD_ACCESS_UNAUTHORISED;
	T.BAD_ADMIN_ERROR;
	T.BAD_AUDIT_OVERFLOW;
	T.BAD_AUDIT_SEQUENCE;
	T.BAD_AUDIT_UNDETECTED;
	T.BAD_AUDIT_UNTRACEABLE;
	T.BAD_DESIGN_COMPLEXITY;
	T.BAD_DESIGN_EXTERNAL;
	T.BAD_DESIGN_SECURITY_FUNCTION_ CORRUPTION;
	T.COVERT_CHANNELS;
	T.MALFUNCTION;
	T.MASQUERADE_BYPASS;
	T.MASQUERADE_HIJACK;
	T.REPUDIATION;
	T.TRAFFIC_ANALYSIS;
	T.TRANSMISSION_ERRORS;
	P.ACCOUNT;
	P.ADMIN_SECURITY_RESTRICTED;
	P.DEFEND;
	P.DUE_CARE;
	P.REMOTE_SECURITY_ADMIN;
		FDP_ACC
		FPT_RVM
		FDP_ACF
		FPT_SEP
		FIA_SOS

TOE$_{OU}$ Objectives	Threats / Policies	Requirements
	P.TOE_USAGE; P.USAGE	

O.PROTECT_ADDRESSES	T.BAD_ACCESS_UNAUTHORISED;
	T.BAD_AUDIT_UNTRACEABLE;
	T.MASQUERADE_BYPASS;
	T.MASQUERADE_HIJACK;
	T.TRAFFIC_ANALYSIS;
	P.DUE_CARE;
	P.PROTECT
	P.RECIPIENTS
		FPR_ANO
		FDP_ACC
		FDP_ACF
		FDP_ETC
		FDP_RIP

O.RELIABLE	T.MALFUNCTION; P.DUE_CARE	FPT_PHP
O.REPLAY_PREVENT	T.BAD_ACCESS_UNAUTHORIZED; P.DUE_CARE	FIA_UID FIA_UAU FPT_STM FPT_RPL

O.SECURE_STARTUP	T.BAD_ACCESS_UNAUTHORISED;
	T.BAD_DESIGN_EXTERNAL;
	T.BAD_PROCEDURES;
	T.MALFUNCTION;
	P.DUE_CARE
		FPT_RCV
		FPT_FLS
		FRU_FLT

O.SECURITY_FUNCTION	T.BAD_ACCESS_INAPPROPRIATE;
	T.BAD_ACCESS_UNAUTHORISED;
	T.BAD_DESIGN_SECURITY_FUNCTION_CORRUPTION;
	T.BAD_PROCEDURES;
	T.COVERT_CHANNELS;
	P.DEFEND;
	P.DUE_CARE;
	P.PROTECT;
	P.TOE_USAGE
		FAU_SAR

O.SELF_TEST	T.ATTACK_DATA;
	T.BAD_ACCESS_INAPPROPRIATE;
	T.BAD_ACCESS_UNAUTHORISED;
	T.BAD_AUDIT_OVERFLOW;
	T.BAD_AUDIT_UNTRACEABLE;
	T.BAD_PROCEDURES;
	T.MALFUNCTION;
	T.MASQUERADE_BYPASS;
	T.MASQUERADE_HIJACK;
	P.DEFEND;
	P.DUE_CARE;
	P.MANAGE;
	P.PROTECT
		FPT_AMT
		FPT_TST
		FRU_FLT
		FPT_PHP
		FIA_SOS

O.SEPARATION	T.BAD_ACCESS_INAPPROPRIATE;
	T.BAD_ACCESS_UNAUTHORISED;
	T.MALFUNCTION;
	P.DUE_CARE
		FDP_RIP
		FPT_SEP

O.TOE_AVAILABLE	T.ATTACK_DATA;
	T.BAD_ACCESS_INAPPROPRIATE;
	T.BAD_ACCESS_UNAUTHORISED;
	T.BAD_ADMIN_ERROR;
	T.BAD_PROCEDURES;
	T.MALFUNCTION;
		FIA_AFL
		FRU_RSA
		FPT_PHP
		FTA_MCS
		FTA_SSL

TOE$_{OU}$ Objectives	Threats / Policies	Requirements

	T.TRANSMISSION_ERRORS;
	P.DEFEND;
	P.DUE_CARE;
	P.PROCEDURES	

O.TOE_USER_ASSOCIATION	T.BAD_ACCESS_INAPPROPRIATE;
	T.BAD_ACCESS_UNAUTHORISED;
	T.PHYSICAL-SECURITY;
	P.DEFEND;
	P.DUE_CARE
	P.RECIPIENTS;
	P.TOE_USAGE;
	P.TSE_CONNECTIONS
	P.USAGE
		FDP_ACF
		FIA_UAU
		FIA_UID
		FDP_ACC
		FIA_USB
		FIA_ATD

O$_{OU}$.IDENTIFY_USER	T.BAD_ACCESS_UNAUTHORISED;
	T.BAD_AUDIT_UNTRACEABLE;
	T.MALFUNCTION;
	T.MASQUERADE_BYPASS;
	T.MASQUERADE_HIJACK;
	T.PHYSICAL_SECURITY
	T.REPUDIATION;
	P.ACCOUNT;
	P.ADMIN_SECURITY_RESTRICTED;
	P.AVAILABLE;
	P.DEFEND;
	P.DUE_CARE;
	P.RECIPIENTS;
	P.REMOTE_SECURITY_ADMIN;
	P.TOE_USAGE;
	P_TSE_CONNECTIONS
	P.USAGE
		FDP_ACC
		FDP_ACF
		FIA_UID
		FIA_UAU
		FIA_USB
		FTA_TSE
		FIA_AFL
		FIA_ATD
		FMT_MOF
		FMT_MSA
		FMT_MTD
		FMT_SMR
		FDP_IFC
		FDP_IFF

O$_{OU}$.SPECIAL_PURPOSE	T.ATTACK_DATA;
	T.BAD_ACCESS_INAPPROPRIATE;
	T.BAD_ACCESS_UNAUTHORISED;
	T.BAD_ADMIN_ERROR;
	P.DUE_CARE
		FPT_SEP

O$_{RU}$.IDENTIFY_USER	T.BAD_ACCESS_UNAUTHORISED;
	T.BAD_AUDIT_UNTRACEABLE;
	T.MALFUNCTION;
	T.MASQUERADE_BYPASS;
	T.MASQUERADE_HIJACK;
	T.PHYSICAL_SECURITY
	T.REPUDIATION;
	P.ACCOUNT;
	P.ADMIN_SECURITY_RESTRICTED;
	P.AVAILABLE;
	P.DEFEND;
	P.DUE_CARE;
	P.RECIPIENTS;
	P.REMOTE_SECURITY_ADMIN;
	P.TOE_USAGE;
	P.TSE_CONNECTIONS
	P.USAGE
		FDP_ACC
		FDP_ACF
		FIA_UID
		FIA_UAU
		FIA_USB
		FTA_TSE
		FIA_AFL
		FIA_ATD
		FMT_MOF
		FMT_MSA
		FMT_MTD
		FMT_SMR
		FDP_IFC
		FDP_IFF

O.ADMIN **The TOE_{OU} must provide functions to enable System and Security Administrators to effectively manage the TOE_{OU} and its security functions, ensuring that only they can access administrative functionality. This objective extends to remote users who are functioning as the administrator at the RU site.**

RATIONALE: The requirement for security alarming (**FAU_ARP**) and its dependency **FAU_SAA**, ensures that properly identified and authenticated administrators are notified of information related to security violations upon detection of a security related alarm, and thereby allows them to properly administer the system.

The requirement for audit data generation (**FAU_GEN**) forms the basis for administrator notification and insures that the level of audit data is selected and the list of data that shall be specified is designated. It also insures that the identity of the individual responsible for the audit event is known.

The requirement for audit review (**FAU_SAR**) insures that audit data can be understood by the reviewer and allows for the designation of what data content may be provided to assigned administrator roles as defined in **FMT_SMR** (e.g. System and Security administrators)

The requirement for selective auditing (**FAU_SEL**) gives the ability for administrators to tailor the reporting of audit data to enhance their ability to analyze security-related events.

The need for System and Security Administrators to I&A themselves to the TOE is accomplished by identifying the administrator based on established password TOE maintained access control list, and strong authentication mechanisms (**FIA_UAU**). Establishment of administrator to TOE session (**FTA_TSE**) and establishing the user's attributes to include their defined role (**FIA_ATD, FPR_UNO**) and inhibiting TSF-mediated actions until the administrator is both properly identified (**FIA_UID**), and authenticated (**FIA_UAU**).

In addition the requirement for handling authentication failures (**FIA_AFL**) specifies requirements which help detect when unauthorized agents are attempting to authenticate themselves as legitimate administrators.

Management of the TSF is restricted to the operations defined in **FMT_MOF**. This is needed to limit the ability to effect changes to functionality or management of security functionality of the TOE to only the System and Security Administrators (**FMT_MTD**) while **FMT_MSA** (and related dependencies **FDP_IFC** and **FDP_IFF**) requirements ensure that values assigned to security attributes are valid w.r.t. a secure state and that default values are appropriately assigned.

The effectiveness of audit data is limited by the administrators' ability to reconstruct sequences of events leading up to and following security related incidences. Establishing the correct sequence of audit events drives the requirement for **FPT_STM** time stamping.

Effective administration is also based on correct interpretation of data exchanges between components of the TOE driven by the **FPT_TDC** requirement.

O.ADMIN_INTERFACE - The TOE must have a friendly set of human interfaces to maximize error free administration.

RATIONALE: The requirement for audit review (**FAU_SAR**) insures that audit data can be understood by the reviewer and allows for the designation of what data content may be provided to assigned administrator roles as defined in **FMT_SMR** (e.g. System and Security administrators)

The requirement for selective auditing (**FAU_SEL**) gives the ability for administrators to tailor the reporting of audit data to enhance their ability to analyze security-related events.

O.ADMIN_SECURITY_REMOTE - The TOE needs to support a secure path capability (providing confidentiality, data integrity, and administrator authentication) to ensure remote administration is performed securely.

RATIONALE: The requirements for remote administration I&A is accomplished as described in **O.ADMIN** with the addition, that remote administrator connectivity will require the establishment of a trusted channel (**FTP_ITC**) between the administrator's remote location and the home TOE. This channel drives the need for the establishment of a session key based on a shared secret which has been generated and verified (**FIA_SOS**) by the connecting TOEs.

Requirements **FCS_CKM** and **FCS_COP** allow for appropriate key management, development of OU to RU connection paths secured with the use of a shared secret and appropriate cryptographic operation.

The access control requirements of **FDP_ACF** ensure that mechanisms are in place that mediate access to audit data based on the security attributes associated with subjects and objects and in the TOEs specific case, in accordance with a defined access control list.

Once again, effective administration is also based on correct interpretation of data exchanges between components of the TOE driven by the **FPT_TDC** requirement.

The need for System and Security Administrators to I&A themselves to the TOE is accomplished by identifying the administrator based on established password TOE maintained access control list, and strong authentication mechanisms (**FIA_UAU**).

O.ADMIN_SEPARATE - The TOE$_{OU}$ and the TOE$_{RU}$ will support two administrative roles, the System Administrator and Security Administrator. The Security Administrator will configure the TOE$_{OU}$ and TOE$_{RU}$ to implement these two separate roles as defined by the site security policy. In addition the Security Administrator will configure all associated RU site TOE$_{RU}$ devices to allow for the authorized RU to perform limited administrative functions.

RATIONALE: The requirements for the TOE to be able to support separate administrator roles is accomplished by the ability to associate defined attributes (**FIA_ATD**) with assigned privileges and authenticate them (**FIA_UAU**).

The binding and association of user attributes with subjects is provided by **FIA_USB**.

The TOE will have separate defined roles (**FMT_SMR**) which will have the ability to perform the functions defined in **FMT_MTD**. These requirements in conjunction with **FMT_MOF** and **FMT_MSA** (and related dependencies **FDP_IFC** and **FDP_IFF**) support the creation, deletion, modification etc. of security attributes and roles and the allocation of responsibilities to these defined roles.

The requirement **FAU_SAR** Restricted Audit Review allows for the possibility of split administrative roles and restrictive distribution of audit data.

The requirement for selective auditing (**FAU_SEL**) gives the ability for administrators to tailor the reporting of audit data to enhance their ability to analyze security related events and allows for the configuration of audit reporting to each of the defined System or Security Administrator roles.

O.ALARM The TOE will be capable of detecting and responding to violations of the site security policy as related to the TOE operation. Violations that are detected either by the TOE or the MD system, which may be attributed to inappropriate operation of the TOE (i.e. internal TOE violations), will be reported to System and Security Administrators, and where appropriate, the AU of RU sites. Violations that may be attributed to inappropriate operation or failures external to the TOE, which are detected by the MD function (i.e. external violations), will also be reported to the same personnel. In either case, upon detection of either an internal or external violation or failure, that cannot be automatically cleared, the TOE will default to a secure state and suspend processing.

RATIONALE: Detection of security related alarms are provided by the requirement for security audit automatic response (**FAU_ARP,** and its dependency **FAU_SAA**) and audit data generation (FAU**_GEN**).

In addition to operational failures, detection of physical attacks may result in an alarm function. This capability results from inclusion of the requirement for passive detection of physical attacks (**FPT_PHP**).

Likewise degraded TOE operation resulting from occurrences such as a power interruption must result in various operations such as back up, suspension of processing, and defaulting to a secure state. The degraded fault tolerance requirement **FRU_FLT** supports these operations.

O.AUDIT **The TOE must provide an audit capability to report security relevant events such that Unauthorized Agents, Authorized Users, System and Security Administrators, actions can be detected and potentially held accountable for their actions. The audit data must be easily understood and be protected from unauthorized modification. Audit events must be selectable.**

RATIONALE: The requirement to inequitably associate AU or Administrators with auditable events is accomplished by preventing these individuals from performing TSF-mediated actions (**FMT_MTD, FMT_MOF**, **FMT_MSA** and related dependencies **FDP_IFC** and **FDP_IFF**) prior to successful identification (**FIA_UID**) and authentication (**FIA_UAU**).

The inclusion of the integrity requirement **(FPT_ITI)** ensures that both authorized user data as well as system generated audit data is protected from unauthorized modification**.**

The requirement **FAU_GEN**, security audit data generation, supports this objective by defining requirements for recording of security relevant events that take place under the control of the TOE security function. **FAU_ARP** (and its dependency **FAU_SAA)**, security alarms define the response to be taken when events indicate a potential security violation.

The requirement **FAU_SEL**, selective audit, directly address this objectives need to have audit event selectable. This requirement gives the ability for administrators to tailor the reporting of audit data to enhance their ability to analyze security related events and allows for the configuration of audit reporting to each of the defined System or Security Administrator roles.

The requirement **FIA_AFL**, authentication failures, supports this objective by ensuring that excessive authentication attempts result in generation of an audit record and notification to System and Security Administrators, thereby thwarting potential unauthorized use.

Effective audit analysis can not be accomplished without time stamping (**FPT_STM**) of audit data so that correct event sequences might be determined. Also, effective audit is also based on correct interpretation of data exchanges between components of the TOE driven by the **FPT_TDC** requirement

O.BACK_UP The TOE must be capable of backing up designated files and configuration parameters automatically. The back up capability must be configurable, based on established site security policy, so that the back up capability could occur upon start-up, shutdown, or after specified periods of usage. The backed up files and parameters will be stored either within the TOE or within another device located within the TSE.

RATIONALE: This objective is satisfied by the inclusion of automated back up capability (**FRU_FLT**) for the TOE security system and configuration files upon detection of loss of power, relevant security faults or violation of security policy, or upon the direction of the MDS.

In addition, the requirement **FAU_GEN**, audit data generation, provides the auditing capability necessary for an administrator to be able to deduce events prior to the occurrence of a system failure and reconstitute system operation in conjunction with the back up system configuration files.

O.CONFIDENTIALITY - The TOE will provide confidentiality by protecting the content of information released from either the OU site or RU site destined to other equivalently privileged users who are also associated with a peer TOE. Upon receipt of protected data, the TOE will remove the confidentiality protection invoked by the transmitting TOE.

RATIONALE: In creating an environment in which data from OU or RU sites is protected, the TOE must be able to:

- generate and destroy cryptographic keys (**FCS_CKM**),
- create and use access control lists (**FDP_ACC**),
- associate users with specific transmissions (**FDP_ACF**), and security attributes (**FDP_ETC, FDP_ITC**),
- maintain confidentiality of the information even after the resources have been made available to others for use (**FDP_RIP**), and
- be able to perform data encryption services (**FCS_COP**).

O.CONNECT Connectivity will be provided only between peer TOEs upon the request of Authorized Users who have been properly identified to their associated TOE. Upon establishment of a TOE-to-TOE connection, the initiating TOE will notify the associated client host equipment that a VPN tunnel has been established.

RATIONALE: The requirement to be able to associate each user with their assigned TOE (**FIA_ATD**) and to provide connectivity based on both mutually authenticated TOEs (**FIA_SOS**) and an access control list, ensures that the O.CONNECT objective is met.

This security objective's resulting mechanism will support the need to restrict connectivity to only peer TOEs upon the request of Authorized Users who have been properly identified (**FIA_UID**) and authenticated (**FIA_UAU**) to their associated TOE.

FCS_CKM and **FCS_COP** support this objective by establishing the parameters upon which TOE peer relationships will be based.

FDP_ACC and **FDP_ACF** access control requirements support O.CONNECT by insuring the provided connectivity between TOEs is based on authorized user assets

With the inclusion of the requirement **FDP_ITC**, import from outside TSF control, the use of an IP address based access control list will control the connectivity provided between authorized users.

O.CRYPTO_SUPPORT - The TOE must interface with cryptographic support mechanisms, which establish files and configuration parameters and insure the integrity of these files and parameters. File examples are: Authorized User registration data, key issuance and revocation lists, access control lists, and assignment of AU privileges files.

RATIONALE: These connectivity requirements are established by two TOE devices being able to establish a security path between each other (**FTP_ITC**) for the exchange of user attributes (**FIA_ATD**) and specification of secrets (**FIA_SOS**). To maintain the integrity of the crypto-support mechanism, a need arises to be able to manage these security parameters (**FMT_MTD**). Also, in order to ensure the integrity of this data, trusted time stamping (**FPT_STM**), consistent interpretation (**FPT_TDC**) and detection of possible data modification (**FPT_ITI**) are all required.

O.HALT The TOE will stop processing data and default to a secure state whenever a failure or insecure operations are detected.

RATIONALE: This objective is addressed by **FRU_FLT** providing the capability for the TOE to stop processing data, generate an audit record (**FAU_GEN**) automatically recover if possible (**FPT_RCV**) and if recovery is not possible, default to a secure state (**FPT_FLS**) whenever a failure or insecure operations are detected (**FAU_ARP** and its dependency **FAU_SAA).**

O.INTEGRITY - The TOE will apply integrity protection to all information it releases to a peer TOE. Upon receipt of protected data the TOE will verify that the received data accurately represents the data that was protected.

RATIONALE: The requirement to apply both integrity and confidentiality protection to user data exported outside the TOE is driven by Export to Outside the TSF Control requirement (**FDP_ETC)** while the requirement to insure the integrity of TSF data is specified in the Integrity of Exported TSF Data (**FPT_ITI).**

Both of these requirements are supported by the inclusion of trusted time stamping **(FPT_STM).**

Verification of imported user data is driven by the requirement Import From Outside TSF Control **(FDP_ITC.)**

O.PROPER_SPEC - The TOE will provide adequately strong security protections to counter the various ways an attack may occur (e.g. The strength of cryptographic algorithms, the length of key, and the design of access control lists must be appropriate for sensitive data and operations.)

RATIONALE: In order to satisfy this security objective, the TOE must have an access control policy (**FDP_ACC**) which is properly enforced and the function of the TSF are non-bypassable (**FPT_RVM**).

Users' associated security attributes must be used to explicitly authorize users access to TOE functionality (**FDP_ACF**).

The separation of the TOE security domain from untrusted subjects is included by the requirement for domain separation (**FPT_SEP.)**

The adequacy of security parameters is defined by the requirement Separation of Secrets **(FIA_SOS).**

O.PROTECT_ADDRESSES - The TOE will protect the confidentiality and integrity of the transmitting and receiving Authorized User's addresses. Upon receipt, the TOE will correctly interpret both originating and destination Authorized User's addresses.

RATIONALE: The requirement Anonymity (**FPR_ANO**) drives the need for the TOE to protect the users' names (actually IP addresses) which are bound to each transmitted datagram.

The implementation of the IPSec network security protocol between TOEs will be used to conceal the originator's IP addresses (which if revealed could be associated with the originating user's name).

The transmitting TOE authentication identity binding will associate the originating RU's asserted address to the received datagram.

This security objective is also supported by the use of an access control policy (**FDP_ACC**).

Access control will be established as defined in the following requirements: **FDP_ACF, FDP_ETC, and FDP_RIP**.

O.RELIABLE The TOE will be reliable with a predicted availability of .97 ("minimal delay" as required for "Mission Support" operations) when operated in a typical office environment.

RATIONALE: From an overt threat by UA to sabotage the functionality of the TOE the functional requirement Passive Detection of Physical Attack (**FPT_PHP**) partially addresses one aspect of the reliability of the TOE.

O.REPLAY_PREVENT - The TOE will prevent access to the TOE and TSE resources from Unauthorized Agents who attempt a replay attack through the TOE by masquerading as an Authorized User.

RATIONALE: User Identification Before an Action (**FIA_UID**) along with the accompanying User Authentication (**FIA_UAU**) as supported by the trusted Time Stamp requirement (**FPT_STM**) support this objective by preventing attempts to use previously successful I&A transactions performed out of sequence by an UA attempting to initiate an unauthorized session.

More directly, this security objective requires the TOE to be resistant to replay attacks as defined in the Replay Detection requirement (**FPT_RPL**).

O.SECURE_START-UP - Upon initial start-up of the TOE or recovery from an interruption in TOE service, the TOE must default to a secure state and not compromise its configuration information, information it is processing, its resources, or information or resources of any connected network.

RATIONALE: Upon detection of a failure or recovery from an interruption the TOE will first attempt to automatically recover (**FPT_RCV**), should recovery not be possible it will return to a secure state.

The preservation of a secure state following failure occurrence is insured by the inclusion of requirement Fail Secure (**FPT_FLS).**

In addition, detection of a degradation in operation will result in an automatic file back-up operation (**FRU_FLT**).

O.SECURITY_FUNCTION - Authorized User's control over TOE security functions will be kept to a minimum.

RATIONALE: The intent of this security objective is addressed by the allocation of roles between System Administrators, Security Administrators and Authorized Users. Assignment of privileges in general is handled outside the functionality of the TOE by supporting trusted security infrastructure components**.**

Explicit exclusion of administrative privileges being assigned to Authorized Users is provided by the requirement **FAU_SAR,** which grants audit review capability to only Authorized Security Administrators.

O.SELF_TEST - The TOE will perform self-tests of its security functions including those required by the site security policy and site procedures.

RATIONALE: Requirements to perform designated self testing during initial start-up, periodically and at the request of an authorized administrator result from the inclusion of the Underlying Abstract Machine Test requirement **(FPT_AMT).**

The ability to test the integrity of both TSF and TSF executable code is driven by the requirement TSF Self Test (**FPT_TST**).

The **FRU_FLT** requirement assumes that periodic self-testing of its security functions will be performed so that upon detection back up will be performed, processing will halt and the TOE will default to a secure state.

The requirement for detection of physical tampering (**FPT_PHP**) typically will result in periodic verification testing of hardware interlocks or keep alive circuitry.

The inclusion of the requirement Specification of Secrets (**FIA_SOS**) drives a self testing need for the TOE to verify the appropriateness of key length, randomness, etc.

O.SEPARATION - The TOE will ensure that residual information from one session does not spill over to another.

RATIONALE: This objective directly drives the inclusion of the Residual Information Protection requirement (**FDP_RIP**) which ensures that previous information doesn't spill over from one allocation of the resource to another.

Additionally, the inclusion of the Domain Separation requirement (**FPT_SEP**) results in the enforcement of domain separation for one subject to another and protection of interference and tampering of untrusted subjects.

O.TOE_AVAILABLE - The TOE will be resilient to denial-of-service attacks.

RATIONALE: Inclusion of the requirement Authentication Failures (**FIA_AFL**) limits the number of unsuccessful authentication attempts coming from individual users' assigned IP addresses, and thereby attempts to address denial-of-service attacks originating from both the high-side and low-side of the network boundary device.

The inclusion of the requirement Resource Allocation (**FRU_RSA**) attempts to control the utilization of the TOE by any individual AU and thereby inhibit denial of service to additional users. This requirement does not address denial-of-service attacks originating on the network low side of the TOE.

Indirectly, inclusion of the TSF Physical Protection requirement (**FPT_PHP**) attempts to inhibit the deliberate sabotage of TOE hardware resulting in denial-of-service to associate AU terminals.

The requirement for Limitation on Multiple Concurrent Session (**FTA_MCS**) allows for the TOE to inhibit an excessive number of sessions to be established between two authorized TOE user's which might result in denial-of-service to other users.

Lastly the requirement Session Locking (**FTA_SSL**) is included to inhibit an established user session which is not being actively utilized from hogging resources that could be otherwise assigned to another user.

O.TOE_USER_ASSOCIATION - The TOE must include a mechanism, which associates all Authorized Users with their assigned site and associated TOE. This mechanism will allow properly identified and authenticated transmitting users to designate only the desired recipient. Based on this mechanism the transmitting TOE will either allow or reject connectivity.

RATIONALE: In order to allow communication between properly identified (**FDP_ACF, FIA_UAU, & FIA_UID**) authenticated users, there must be an access control policy that is properly enforced (**FDP_ACC**). To help in enforcing this policy user's identities and their transmitted data (**FIA_USB**) will be bound together and must be associated with their security attributes (**FIA_ATD**).

O$_{OU}$.IDENTIFY_USER - Usage of the TOE$_{OU}$ will be continuously restricted to only properly identified Authorized Users, and System or Security Administrators. Identification of Authorized Users may minimally be based on an asserted IP address and correct password. Identification of System or Security Administrators will be based on the use of hardware tokens

RATIONALE: This objective is a mandate for the specified access control policy (**FDP_ACC**) using attribute based access control (**FDP_ACF**) with the requirement that users identify themselves before use of the TOE$_{OU}$ resources (**FIA_UID, FIA_UAU**).

It also requires that use of the TOE$_{OU}$ is continuously restricted to authorized users who are re-authenticated for each transmission, and that users' security attributes are bound to them (**FIA_USB**).

In addition the TOE must be able to restrict the establishment of user sessions based on invalid user parameters (**FTA_TSE**).

Additional contributing requirements include the need to handle authentication failures (**FIA_AFL**) and the maintenance of user attributes by the TSF (**FIA_ATD**) as well as the management of security data (**FMT_MOF, FMT_MSA, FMT_MTD, FMT_SMR** and related dependencies **FDP_IFC** and **FDP_IFF**.)

O$_{OU}$.SPECIAL_PURPOSE - The TOE$_{OU}$ is a Special Purpose Device (definition previously provided in Terminology section) and consequently will not execute general-purpose programs.

RATIONALE: This security objective will largely be supported by functional requirements associated with the TSE rather than the TOE. The only resulting requirement for the TOE itself is the need for the TOE to support Domain Separation (**FPT_SEP**) for one subject to another and protection of interference and tampering of untrusted subjects.

O$_{RU}$.IDENTIFY_USER - Usage of the TOE$_{RU}$ will be continuously restricted to only properly identified Remote Users, and System or Security Administrators. Identification of Remote Users and System or Security Administrators will be based on the use of hardware tokens.

RATIONALE: This objective is a mandate for the specified access control policy (**FDP_ACC**) using attribute based access control (**FDP_ACF**) with the requirement that users identify themselves before use of the TOE_{RU} resources (**FIA_UID, FIA_UAU**).

It also requires that use of the TOE_{RU} is continuously restricted to authorized users who are re-authenticated for each transmission, and that users' security attributes are bound to them (**FIA_USB**).

In addition the TOE must be able to restrict the establishment of user sessions based on invalid user parameters (**FTA_TSE**).

Additional contributing requirements include the need to handle authentication failures (**FIA_AFL**) and the maintenance of user attributes by the TSF (**FIA_ATD**) as well as the management of security data (**FMT_MOF, FMT_MSA, FMT_MTD, FMT_SMR** and related dependencies **FDP_IFC** and **FDP_IFF**.)

6.3 Argument that EAL 3 is Appropriate

The VPN PP development team chose EAL-3 after a long and detailed analysis of the types of data we were trying to protect, the robustness of mechanisms that are available in today's development environment, the threats that we documented, and the associated risks involved. We sought out as much guidance and expertise as possible and found several sources that aided considerably in arriving at our final decision. The Information Assurance Technical Framework (IATF) has a Robustness Strategy section that we referenced thoroughly. We also sought out guidance in the Common Criteria and other emerging documents such as the Guidance and Policy for "Department of Defense Global Informatin Grid Information Assurance" (commonly referred to as the GIG) memorandum No. 6-8510. Lastly, we conducted interviews with several consultants who, based upon current testing, have developed an expertise as to what current commercial products are capable of providing.

Based on this analysis the team eventually became comfortable with the notion that most organizations are able to relate the importance of their data to three subjective categories with corresponding requirements for three assurance levels of IT products or subsystems ...low, medium and high importance. Organizations in and out of governmental circles may call each of these categories different names, but they tend to distinguish among three.

Based on the team's understanding of User requirements we were attempting to address, we decided to focus on the medium level robustness and strength of security mechanisms which, in a DoD context are appropriate for the protection of sensitive data applicable for "Mission Support" operations. Mission Support data is defined as sensitive data which may be important to the support of deployed contingency forces, must be absolutely accurate, but can sustain minimal delay without seriously affecting operational readiness. The PP team believes that requirements specified in this PP are appropriate in public or private, non-DoD environments for the protection of both administrative information and information related to sensitive, day-to-day operations. This PP defines the security functional and assurance requirements, which are appropriate to protect these classes of data in both DoD and private sector applications.

The specific customer requirements the PP team is attempting to address is a Navy customer that defined the information they needed to protect as, "Ordinary personnel, medical, financial, and investigatory records and other records judged to be of comparable sensitivity. The PP team recognized that such data is very sensitive to any organization and its personnel, but not as sensitive as data at the highest level, which this same customer viewed as "If disclosed or modified improperly could threaten an individual's life." Therefore, the data upon which the PP team focused was that which was higher than routine, but not as crucial as to threaten the organization’s, or personnel there-in’s, ability to survive.

Based on our analysis of the IATF's Robustness Strategy we were guided to choose an information value of 3 (V3) and a threat level of either 4 or 5 (T4 or T5). "V3: Violation of the information protection policy would cause some damage to the security, safety, financial posture, and/or infrastructure of the organization." T4 and T5 specify that the adversary is sophisticated and has moderate resources. The only difference between the two is that T4's adversary is willing to take little risk; whereas T5's is willing to take significant risk.

Using the above guidance led us to an EAL-3 and Strength of Mechanism Level
2 (SML-2). SML is discussed in detail in Section 6.4.

EAL-3 provides for methodically tested and checked mechanisms. It permits a conscientious developer to gain maximum assurance from positive security engineering at the design stage without substantial alteration of existing sound development practices. This level is applicable, by definition, in circumstances where developers or users require a moderate level of independently assured security, and require a thorough investigation of the TOE and its development without substantial re-engineering. The Common Criteria, Part 3, "Security Assurance Requirements," has a complete definition of EAL-3.

Additionally, we thought it important to include an additional assurance requirement, ADV_SPM.1. This requirement calls for the developer to produce an informal TOE security policy (TSP) model. The TSP forms a set of rules that regulate how assets are managed, protected, and distributed within the TOE. Because of the critical security function this TOE provides, we added this requirement to assure ourselves that a developer had a well thought out set of rules that regulate how TOE assets are managed, protected, and distributed. We did not wish to burden the developer with formally stating this policy, because our focus was on medium rather than a high level of data importance.

6.4 Minimum Strength of Function Arguments

The VPN Protection Profile development team chose Strength of Mechanism Level 2 (SML2) after reviewing the guidance on this issue found in the Information Assurance Technical Framework's (IATF) Robustness Strategy (RS) document. The RS does not pretend to be the definitive word on this subject. It states, "The Strategy is still being formulated and the tables are not considered complete or adequately defined." The intent of the RS is to ensure that mechanisms across security services at the same strength level provide comparable protection, in that they encounter equivalent threats. Strength levels are relative measures of effort and cost required, and all things being equal, especially cost, the highest strength mechanism should always be chosen. Using this guidance we were quickly convinced to choose SML2.

The FCS (Cryptographic Support) Class in the Protection Profile contains a complete set of functions from key generation through key destruction. We have been very specific about which mechanisms we recommend for each of these cryptographic functions. Basically, the mechanisms listed and there strengths were chosen after deliberating on the value of the data we were trying to protect. The discussion we presented in 6.3 is pertinent in this strength of mechanism (SOM) discussion as well. By discussing data that falls into three general protection/sensitivity levels (low, medium and high) and STARTING with which encryption bit length is required presently to adequately protect medium sensitive data, the remaining requirements fell into place. Concerning the bit length requirement for cryptographic operation, low and medium level data should be adequately protected by at least 112 bits of security and high level data by the yet undefined AES at some higher, and presently, undetermined bit length. Once we chose 112 bit 3DES for cryptographic operation, we chose "matching" mechanisms (as well as we could) for the remaining mechanisms.

The use of 3DES, which generally takes 112 bit keys, may be confusing here. The effective strength of the IPSec 3DES implementation is currently limited by the size of the Diffie-Hellman group. That is because the key that is used in this 3DES implementation is generated from the Diffie-Hellman key exchange. Diffie-Hellman uses 1024 bit primes which translates to 80 bits of security. When one upgrades to the newly added 1536 bit IPSec group, the effective SOM increases to approximately 96 bits of security. When IPSec uses the NIST elliptic curves with the Diffie-Hellman key exchange, the full 112-bit strength of the 3DES will be achieved.

6.5 Dependency Rationale

6.5.1 Dependency Analysis

Table 7 Functional Security Requirement Dependency Analysis

Index	Requirement	Dependencies	Coverage (Index Number)
1	FAU_ARP.1	FAU_SAA.1	Not covered. Ref. 6.5.2
2	FAU_GEN.1	FPT_STM.1	46
3	FAU_SAR.1	FAU_GEN.1	2
4	FAU_SAR.2	FAU_SAR.1	3
5	FAU_SEL.1	FAU_GEN.1 FMT_MTD.1	2 31
6	FCS_CKM.1	FCS_CKM.2 or FCS_COP.1 FCS_CKM.4 FMT_MSA.2	7 9 8 29
7	FCS_CKM.2	FDP_ITC.1 or FCS_CKM.1 FCS_CKM.4 FMT_MSA.2	 6 8 29
8	FCS_CKM.4	FDP_ITC.1 or FCS_CKM.1 FMT_MSA.2	 6 29
9	FCS_COP.1	FDP_ITC.1 or FCS_CKM.1 FCS_CKM.4 FMT_MSA.2	 6 8 29
10	FDP_ACC.2	FDP_ACF.1	11
11	FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	10 30
12	FDP_ETC.1	FDP_ACC.1 or FDP_IFC.1	10
13	FDP_ETC.2	FDP_ACC.1 or FDP_IFC.1	10
14	FDP_ITC.2	FDP_ACC.1 or FDP_IFC.1 FTP_ITC.1 or FTP_TRP.1 FPT_TDC.1	10 54 47
15	FDP_RIP.2	None	--

16	FIA_AFL.1	FIA_UAU.1	20
17	FIA_ATD.1	None	--
18	FIA_SOS.1	None	--
19	FIA_SOS.2	None	--
20	FIA_UAU.2	FIA_UID.1	25
21	FIA_UAU.3	None	--
22	FIA_UAU.5	None	--
23	FIA_UAU.6	None	--
24	FIA_UAU.7	FIA_UAU.1	20
25	FIA_UID.2	None	--
26	FIA_USB.1	FIA_ATD.1	17
27	FMT_MOF.1	FMT_SMR.1	34
28	FMT_MSA.1	FDP_ACC.1 or FDP_IFC.1 FMT_SMR.1	12 34
29	FMT_MSA.2	ADV_SPM.1 FDP_ACC.1 or FDP_IFC.1 FMT_MSA.1 FMT_SMR.1	A18 (table 6.4) 10 27 33
30	FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	28 34
31	FMT_MTD.1	FMT_SMR.1	34
32	FMT_MTD.2	FMT_MTD.1 FMT_SMR.1	31 34
33	FMT_MTD.3	ADV_SPM.1 FMT_MTD.1	A18 (table 6.4) 31
34	FMT_SMR.2	None	--
35	FMT_SMR.3	FMT_SMR.1	34
36	FPR_ANO.1	None	--
37	FPR_UNO.4	None	--
38	FPT_AMT.1	None	--
39	FPT_FLS.1	ADV_SPM.1	A18 (table 6.4)
40	FPT_ITI.1	None	--
41	FPT_PHP.1	FMT_MOF.1	27
42	FPT_RCV.2	FPT_TST.1 AGD_ADM.1 ADV_SPM.1	48 A8 (table 6.4) A18 (table 6.4)
43	FPT_RPL.1	None	--
44	FPT_RVM.1	None	--
45	FPT_SEP.1	None	--
46	FPT_STM.1	None	--
47	FPT_TDC.1	None	--
48	FPT_TST.1	None	--
49	FRU_FLT.1	FPT_FLS.1	39

50	FRU_RSA.1	None	--
51	FTA_MCS.1	FIA_UID.1	25
52	FTA_SSL.3	None	--
53	FTA_TSE.1	None	--
54	FTP_ITC.1	None	--

Table 8 Assurance Requirement Dependencies

Index	Requirement	Dependencies	Coverage
A1	ACM_CAP.3	ACM_SCP.1 ALC_DVS.1	A2 A10
A2	ACM_SCP.1	ACM_CAP.3	A1
A3	ADO_DEL.1	None	--
A4	ADO_IGS.1	AGD_ADM.1	A8
A5	ADV_FSP.1	ADV_RCR.1	A7
A6	ADC_HLD.2	ADV_FSP.1 ADV_RCR.1	A5 A7
A7	ADV_RCR.1	None	--
A8	AGD_ADM.1	ADV_FSP.1	A5
A9	AGD_USR.1	ADV_FSP.1	A5
A10	ALC_DVS.1	None	--
A11	ATE_COV.2	ADV_FSP.1 ATE_FUN.1	A5 A13
A12	ATE_DPT.1	ADV_HLD.1 ATE_FUN.1	A6 A13
A13	ATE_FUN.1	None	--
A14	ATE_IND.2	ADV_FSP.1 AGD_ADM.1 AGR_USR.1 ATE_FUN.1	A5 A8 A9 A13
A15	AVA_MSU.1	ADO_IGS.1 ADV_FSP.1 AGD_ADM.1 AGD_USR.1	A4 A5 A8 A9
A16	AVA_SOF.1	ADV_FSP.1 ADV_HLD.1	A5 A6
A17	AVA_VLA.1	ADV_FSP.1 ADV_HLD.1 AGD_ADM.1 AGD_USR.1	A5 A6 A8 A9
A18	ADV_SPM.1	ADV_FSP.1	A5

6.5.2 Rationale for not satisfying all dependencies

For both the TOE_{OU} and the TOE_{RU}, requirement FAU_ARP.1.1 of Class FAU Security Audit has been specified and has the dependency for requirement FAU_SAA.1 to be considered for inclusion. This dependency requirement has not been included in either of the TOE requirement sets because we are requiring the TOE to only report (read out) audited events and not perform any analysis. FAU_SAA.1 calls for a single rule based audit analysis capability, which is not a requirement of either the TOE_{OU} or TOE_{RU}.

6.6 Mutually Supportive and Internally Consistent Requirements

This section provides arguments that the TOE_{OU} and TOE_{RU} requirements form a mutually supportive and internally consistent whole.

6.6.1 Overview

Typical VPN solutions, when deployed in the context of a protected system-high enclave architecture with isolated remote users, have a natural decomposition into two distinct functions. The first is the client function associated with the authorized VPN user's workstation, and the second is the server function typically associated with enclave boundary components.

This protection profile has considered each of these VPN functions appropriately deployed into three different physical security environments.

We call the first environment an Operational User (OU) site and it represents the typical location for the majority of VPN users. An OU site may be thought of as a system-high enclave configuration, which is isolated from the public network by the installation of security boundary protection mechanisms. In this physical configuration, the client application resident on individual users' workstations typically has minimal functionality due to the allocation of most VPN functionality in the VPN server security boundary functionality. However, in some user implementations a complete VPN client may also be included on users workstations providing the capability for establishment of Communities of Interest (COIs) among privileged users (e.g. the finance department business area segregated from the general community of employees).

We call the second environment a Regional Service Center (R/SC). (Many network architectures do not contain a R/SC). The R/SC location typically has no VPN users resident. Its main purpose is to allow network designers the capability of stripping off the VPN security protections for one or two purposes.

- It allows the examination or processing of the composite plain-text user data. We refer to this as *Misuse Detection* in the PP. It includes virus detection, intrusion detection, and other such security applications.

- It allows for the interconnection of non-interoperable security systems by decrypting and then allowing for the switching of plain text between systems.

For purposes of this analysis we assume that the R/SC VPN function is logically the same as the VPN server application analyzed as part the OU site configuration. Consequently, the required security functional and assurance requirements of the R/SC will be logically consistent to those of the OU site.

The third environment considered is referred to as the Remote User (RU) site and represents the typical environment for traveling users who are deployed away from their home OU site but still require access to the information resident within their home site. Our analysis considered the additional threat associated with deployment away from the physical environment of a typical system-high enclave, and attempts to address issues such as occasional need to leave the equipment unattended while still preserving access control to network resources or lack of local network administration and monitoring.

The effectiveness of the specified security functional requirements allocated to the VPN functions at the OU and RU sites have been thoroughly rationalized in section 6 of this PP. In section 6.1 of our analysis we have traced the mapping of relevant security threats and policies to security objectives, which take into consideration applicable assumptions. Then subsequently, in section 6.2 our analysis maps the identified security objectives to the specific security functional requirements that have been detailed in sections 5.1 and 5.2 of the PP as applicable to the OU and RU site environments.

6.6.2 Semantics of Coverage Analysis

The security needs addressed by this PP result from considering the stated security policies and perceived threats. We did not confine the breadth of considered policy and threat based on the value of the data involved. Specifically, the information value addressed by this PP is characterized as sensitive, which is defined as information that has been deemed as important, the loss of which might cause financial difficulties, schedule impacts or affect personnel well-being. However, the totality of the threat considered in this PP has purposefully been broad and inclusive. Rather than temper the identified threats with the consideration as to the likelihood that an adversary would mount that level of attacks against a limited value target, we preferred to consider all threats we could think of. Then we specified requirements we thought appropriate in the detailed functional and assurance requirements sections.

Therefore, in sections 3.1 and 3.2 the identified threats and policies are assumed to be applicable to all of the TOE security environments (OU site, RS/C and RU site) identified in the preliminary analysis. The differentiation between environments identified in our analysis is reflected in the details of applicable assumptions. We differentiated among applicable assumptions in section 3.3. The differences resulting from TOE environments resulted in itemized lists of assumptions applicable to **both** the OU and RU sites as well as lists of assumptions applicable to only **one** of each type of site.

6.6.3 Identification of TOE Requirements

Each of the TOE security functional requirements (SFR's) detailed in this PP (sections 5.1 and 5.2) are drawn from Part 2 of the Common Criteria (CC). The identifiers (e.g. FAU – Security Audit) for these SFRs are based on the CC identifiers. Section 5.1 of this PP identifies the SFRs applicable to the Operational User site TOE (TOE_{OU}), while section 5.2 itemizes the SFRs applicable to the Remote User site TOE (TOE_{RU}).

Operations have been carried out on each CC-derived SFR following CC guidelines for specification of assignments, selections, refinements, and iterations, and are used to customize the generic CC SFRs making them specifically applicable to the security environments and objectives of this PP. The conventions used to identify these operations in the text of the SFRs are explained under the heading "Conventions" in the beginning of this PP.

This PP specifies assurance requirements for the system as a whole. The security assurance requirements were derived from Part 3, Version 2, of the CC. The overall assurance level for the system is EAL3 with the addition of component ADV_SPM.1, Informal TOE Security Policy Model.

6.6.4 Compatible Functionality of the SFRs

All classes of SFRs defined within the CC have been included in the specification of both the TOE_{OU} and TOE_{RU}. In addition, all SFR dependencies defined by the CC have been included in these TOE specifications.

6.6.5 TOE Assumptions, ITRs, and NITRs Coherency

The assumptions made in this analysis are all based on realistic common security practices and expectations. For example, rather than assume away the possibility of system administrators subverting the protection typically provided by the system, based on historical evidence of lack of trustworthy behavior by some administrators or insiders placed in positions of unlimited trust (e.g. crypto-custodian gone bad), the PP has attempted to specify SFRs that would mitigate this inherent risk. For example two-person control provided by the dual roles of System and Security administrators.

On the other hand, derivation of TOE environmental requirements are driven by the set of assumptions which limit the required functionality of the TOE and place requirements on other components within the security environment. For instance, it is assumed that the TOE will generate audit events and ship them to a centralized Misuse Detection system for analysis and alarm detection and responsive action. Likewise, elements external to the TOE are counted on to provide sufficient cryptographic support, communication channel availability, training, maintenance and restore capabilities.

Therefore, the combination of SFRs placed on the TOE along with requirements placed on TSE components derived from the assumptions itemized in section 3.3.1 together address the needs of the defined threats and policies.

6.6.6 SFRs Grounding in Objectives

All the security functional requirements identified in sections 5.1 and 5.2 of the PP have a basis in the security objectives related to each of the TOE environments (TOE_{OU} and TOE_{RU}), as is shown in Table 9 below:

Table 9 TOE Functional Security Requirements Mapping to Security Objectives

REQUIREMENT	OBJECTIVES
FAU_ARP	O.ADMIN O.ADMIN_SECURITY_REMOTE O.ALARM O.AUDIT O.HALT
FAU_GEN	O.ADMIN O.ADMIN_SECURITY_REMOTE O.ALARM O.AUDIT O.BACK_UP O.HALT
FAU_SAA.1	O.ADMIN O.ADMIN_SECURITY_REMOTE O.ALARM O.AUDIT O.HALT
FAU_SAR	O.ADMIN O.ADMIN_INTERFACE O.ADMIN_SECURITY_REMOTE O.ADMIN_SEPARATE O.SECURITY_FUNCTION
FAU_SEL.1	O.ADMIN O.ADMIN_INTERFACE O.ADMIN_SECURITY_REMOTE O.ADMIN_SEPARATE O.AUDIT

REQUIREMENT	OBJECTIVES
FCS_CKM	O.ADMIN_SECURITY_REMOTE O.CONFIDENTIALITY O.CONNECT
FCS_COP.1	O.ADMIN_SECURITY_REMOTE O.CONFIDENTIALIY O.CONNECT
FDP_ACC.2	O.CONFIDENTIALIY O.CONNECT O_{OU}.IDENTIFY_USER O.PROPER_SPEC O.PROTECT_ADDRESS O.TOE_USER_ASSOCIATION
FDP_ACF.1	O.ADMIN_SECURITY_REMOTE O.CONFIDENTIALITY O.CONNECT O_{OU}.IDENTIFY_USER O.PROPER_SPEC O.PROTECT_ADDRESS O.TOE_USER_ASSOCIATION
FDP_ETC	O.CONFIDENTIALITY O.INTEGRITY O.PROTECT_ADDRESS
FDP_IFC.1	O.ADMIN O.ADMIN_SECURITY_REMOTE O.ADMIN_SEPARATE O.AUDIT O_{OU}.IDENTIFY_USER
FDP_IFF.1	O.ADMIN O.ADMIN_SECURITY_REMOTE O.ADMIN_SEPARATE O.AUDIT O_{OU}.IDENTIFY_USER
FDP_ITC.2	O.CONFIDENTIALITY O.INTEGRITY O.CONNECT
FDP_RIP.2	O.CONFIDENTIALITY O.PROTECT_ADDRESS O.SEPARATION
FIA_AFL.1	O.ADMIN O.ADMIN_SECURITY_REMOTE O.AUDIT O_{OU}.IDENTIFY_USER O.TOE_AVAILABLE
FIA_ATD.1	O.ADMIN O.ADMIN_SECURITY_REMOTE

REQUIREMENT	OBJECTIVES
	O.ADMIN_SEPARATE O.CONNECT O.CRYPTO_SUPPORT O.TOE_USER_ASSOCIATION O_{OU}.IDENTIFY_USER
FIA_SOS	O.ADMIN_SECURITY_REMOTE O.CONNECT O.CRYPTO_SUPPORT O.PROPER_SPEC O.SELF_TEST
FIA_UAU	O.ADMIN O.ADMIN_SECURITY_REMOTE O.ADMIN_SEPARATE O.AUDIT O.CONNECT O_{OU}.IDENTIFY_USER O.REPLAY_PREVENT O.TOE_USER_ASSOCIATION
FIA_UID.2	O.ADMIN O.ADMIN_SECURITY_REMOTE O.AUDIT O.CONNECT O.TOE_USER_ASSOCIATION O_{OU}.IDENTIFY_USER O.REPLAY_PREVENT
FIA_USB.1	O.ADMIN_SEPARATE O_{OU}.IDENTIFY_USER O.TOE_USER_ASSOCIATION
FMT_MOF.1	O.ADMIN O.ADMIN_SECURITY_REMOTE O.ADMIN_SEPARATE O.AUDIT O_{OU}.IDENTIFY_USER
FMT_MSA	O.ADMIN O.ADMIN_SECURITY_REMOTE O.ADMIN_SEPARATE O.AUDIT O_{OU}.IDENTIFY_USER
FMT_MTD	O.ADMIN O.ADMIN_SECURITY_REMOTE O.AUDIT O.CRYPTO_SUPPORT O_{OU}.IDENTIFY_USER
FMT.SMR	O.ADMIN O.ADMIN_INTERFACE

REQUIREMENT	OBJECTIVES
	O.ADMIN_SECURITY_REMOTE O.ADMIN_SEPARATE O_{OU}.IDENTIFY_USER
FPR_ANO.1	O.PROTECT_ADDRESS
FPR_UNO.4	O.ADMIN O.ADMIN_SECURITY_REMOTE
FPT_AMT.1	O.SELF_TEST
FPT_FLS.1	O.HALT O.SECURE_STARTUP
FPT_ITI.1	O.AUDIT O.CRYPTO_SUPPORT
FPT_PHP.1	O.ALARM O.TOE_AVAILABLE O.RELIABLE O.SELF_TEST
FPT_RCV.2	O.HALT O.SECURE_STARTUP
FPT_RPL.1	O.REPLAY_PREVENT
FPT_RVM.1	O.PROPER_SPEC
FPT_SEP.1	O.PROPER_SPEC O_{OU}.SPECIAL_PURPOSE
FPT_STM.1	O.ADMIN O.ADMIN_SECURITY_REMOTE O.AUDIT O.CRYPTO_SUPPORT O.INTEGRITY O.REPLAY_PREVENT
FPT_TDC.1	O.ADMIN O.ADMIN_SECURITY_REMOTE O.AUDIT O.CRYPTO_SUPPORT
FPT_TST.1	O.SECURE_STARTUP
FRU_FLT.1	O.ALARM O.BACK_UP O.CRYPTO_SUPPORT O.SECURE_STARTUP O.SELF_TEST
FRU_RSA.1	O.TOE_AVAILABLE
FTA_MCS.1	O.TOE_AVAILABLE
FTA_SSL.3	O.TOE_AVAILABLE
FTA_TSE.1	O.ADMIN O.ADMIN_SECURITY_REMOTE O_{OU}.IDENTIFY_USER
FTP_ITC.1	O.ADMIN_SECURITY_REMOTE

REQUIREMENT	OBJECTIVES
	O.CRYPTO_SUPPORT

Appendix A — Common Criteria Acronyms

CC	Common Criteria
EAL	Evaluation Assurance Level
IT	Information Technology
PP	Protection Profile
SF	Security Function
SFP	Security Function Policy
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSFI	TSF Interface
TSP	TOE Security Policy

Appendix B: Auditable Events and Misuse Detection (MD)

Comments and Rationale:

The generation of audit records, audit analysis, and audit reporting are complex processes that must support the security policy of the organization. As has been previously stated, Virtual Private Network (VPN) products compliant with this Protection Profile (PP) must be capable of generating audit records and relaying these records to an external Misuse Detection (MD) system for subsequent audit analysis. In addition, compliant VPN products must be capable of reacting to various commands issued by the MD system and taking preventative actions such as halting processing. The VPN PP has attempted to document what a compliant VPN product must do in the way of audit record generation and reporting, while this appendix attempts to specify what action and events will result in a VPN product audit record. In putting together this list of actions and events which result in the generation of a VPN product audit record, the team has reviewed several documents on this subject and examined several products currently available in the marketplace. However, we do not pretend this analysis is complete. This list of auditable events is subject to change depending upon the actual environment in which the VPN product is to operate and the specific approach to audit that individual vendors will propose in associated Security Targets (STs). In this appendix the Goal VPN PP team has attempted to generalize the list of auditable events so that a product vendor may have a degree of latitude in specifying how their specific product addresses the overall audit requirements. Therefore, this list of required audit event reporting may not be exact nor is it necessarily complete. The acceptability of individual product's audit reporting is determined by the evaluation of specific products against their associated Security Targets.

The overall goal for system security auditing is to detect auditable events, generate audit records, reliably provide them to an audit analysis tool, and appropriately react to both failures and attacks identified by the audit analysis tool, which is normally external to the TOE. In the proposed system architecture the audit analysis task has been removed from proposed VPN products and allocated to an associated MD system. The MD system analysis may indicate event activities and behavior patterns that could be considered security threats to the computer system and/or network. Please note that we have stated in the past, and will do so again for emphasis, that MD systems, including intrusion detection, are intended to protect the IT environment from BOTH the insider and outsider threats. All too often intrusion detection tools are viewed to protect the environment from the outsider threat only.

The setup, maintenance and analysis of the audit subsystem and event logs is tedious and error-prone and, without third-party tools, all but impossible. This appendix details our auditing recommendations, which are made without regard to the difficulty of achieving them. Some of the recommendations are "best case" with regards to security, but not to cost or complexity of implementation. Appropriate third-party tools will significantly reduce this cost and complexity, rendering these recommendations feasible. We have assumed that the MD system will perform much of the auditing function. We also assume that devices throughout the TSE are sending audit records to a secure location within the MD system for analysis. The TOE and other devices in the system generate audit records based on System and Security Administrators' selection and programming of the TOE.

Effective auditing is a tradeoff between level of security, system overhead, and complexity of the analysis of the audit trail. In many cases, administrators audit far too little, because the combination of high system overhead and complex analysis overshadow the security benefits. In order to achieve higher security through auditing, one must create a policy that generates relevant data, minimizes system overhead, and is consistent across the enterprise, or the enterprise runs the very real risk that administrators simply won't audit at all. Only with relevant audit data as input can one proceed to the next step of collecting and analyzing all log files in the enterprise and correlating events and patterns that span multiple machines.

Historically, auditing has always been done on a per-machine basis. No thought was given to the redesign of auditing subsystems when networking was introduced. In order to obtain the most information from auditing in an enterprise, the data must be collected and analyzed centrally by modern MD systems in order to spot trends and behaviors that may be occurring between machines. For instance, consider a sensitive file that exists on multiple machines. A user may have permission to access this file on all machines. If the user's behavior pattern is such that the file is accessed once a day on the local machine, and that pattern suddenly changes to one whereby the user accesses the file on ten other machines in the network within an hour, there might be cause for concern. Only with enterprise-wide audit analysis of *positive* (allowed) events will this behavior be spotted.

The first order of business is generating a relevant audit policy (many organizations have never produced such a policy). This audit policy must be clearly specified and incorporated into the applicable written security policy. In order for the organization to implement this policy, it must be distributed to all computers on the network**.** The written policy must address the size of the audit log file and the method of protecting it within the TSE.

Note that this PP does not specify a format or standard language or protocol for audit records, because no such standard (actual or defacto) exists presently. Each vendor should specify their audit record format based on the current best available commercial practice when they decide on the audit logging details and identify their implemented format in the product's associated Security Target. The MD system must understand whatever format the vendor chooses. It should be very user friendly so that administrators can easily tune and use the features of this security system. Therefore, the organization must carefully choose security components to match the capabilities of the MD system chosen and vice versa.

The MD system should have the ability to:

- Automatically notify an administrator or otherwise respond when an event occurs;
- Detect and respond to a group of events, known as *data source authentication data or integrity protection information;*
- Analyze and view an aggregate of event logs from multiple machines;
- Understand event details. Often there are many events that actually make up an operating system action, and the administrator must sift through many “noisy” entries in order to figure out what action really occurred.
- “Data mine” the event logs. There should be ad-hoc query/reporting tools that allow post-facto analysis of the data.
- Notify the associated VPN product when the result of the audit analysis indicates that the accumulation of audit records warrant the termination of VPN operation.

These features of the MD system will enable management to realize the true potential of auditing. To use the audit logs as a part of an effective security policy, a combination of the following must be employed:

- Centralized administration and storage of enterprise audit records.
- Real-time analysis of log data, with administrator notification and/or automatic response when pre-defined data (authentication) is logged.
- Correlation of enterprise-wide log data.
- Data mining operations with appropriate query and reporting functionality.

The TOE Shall Generate Audit Records upon detection of the following:

1. **All TOE file and object accesses**

   Recording of this auditable event cannot be switched off by administrators (i.e., not tunable).

   This event includes administration and group management auditing checks against authorizes and unauthorized changes to TOE databases

   Audit records resulting from this audit event contains the following detail:
   - time of access;
   - identity of requester (IP address);
   - success or failure code of access;
   - facility source (domain name, if available);
   - severity code;
   - event identifier.

2. **All TOE use (not including administration)**

   Successful login, failed login, correct response to introduction challenge are included. Numerous repeat login attempts could mean an attempted attack on your security domain.

   Recording of this auditable event may be switched on or off (or tuned) by the Security Administrator.

   Audit records resulting from this audit event contains the following detail:
   - time of use;
   - identity of user (IP address);
   - success or failure code of use;
   - facility source (domain name, if available);
   - severity code;
   - event identifier.

3. **Wrong password or token given**

   The ability to select a relative number of unsuccessful password attempts will be granted to the Security administrator.

   Audit records resulting from this audit event contains the following detail:
   - time of use;

- identity of user (IP address);
- facility source (domain name, if available);
- event identifier.

4. **Message type from remote address, specific ports, or domain identifier do not match authorized lists**

Recording of this auditable event cannot be switched off by administrators, (i.e., not tunable).

Audit records resulting from this audit event contains the following detail:

- time of access;
- identity of requester (IP address);
- facility source (domain name, if available);
- severity code;
- event identifier.

5. **Message type from remote address or domain does not match session list**

Recording of this auditable event cannot be switched off by administrators (i.e., not tunable).

Audit records resulting from this audit event contains the following detail:

- time of access;
- identity of requester (IP address);
- facility source (domain name, if available);
- severity code;
- event identifier.

6. **Bad “establish/reply” occurrence from IP *address or domain name***

Recording of this auditable event cannot be switched off by administrators, (i.e., not tunable).

Audit records resulting from this audit event contains the following detail:

- time of occurrence;
- identity of requester (IP address);
- facility source (domain name, if available);
- severity code;
- event identifier.

7. **Internal encryption/decryption or compress/decompress error from address**

Recording of this auditable event cannot be switched off by administrators (i.e., not tunable).

Audit records resulting from this audit event contains the following detail:

- time of occurrence;
- identity of requester (IP address);
- facility source (domain name, if available);
- severity code;
- event identifier.

8. **Internal integrity check error from address**

Recording of this auditable event cannot be switched off by administrators, (i.e., not tunable).

Audit records resulting from this audit event contains the following detail:

- time of occurrence;
- identity of requester (IP address);
- facility source (domain name, if available);
- severity code; event identifier.

9. **Internal packet length error from address**

Recording of this auditable event cannot be switched off by administrators, (i.e., not tunable).

Audit records resulting from this audit event contains the following detail:

- time of occurrence;
- identity of requester (IP address);
- facility source (domain name, if available);
- severity code;
- event identifier.

10. **Maximum number of clients exceeded**

Recording of this auditable event cannot be switched off by administrators (i.e. not tunable).

Audit records resulting from this audit event contains the following detail:

- time of occurrence;
- identity of requester (IP address);
- facility source (domain name, if available);
- severity code;

- event identifier.

11. **Specific violations of the site security policy**.

The TOE must have a facility that enables the Security Administrator to create ad hoc audit log events. This will allow the administrator to structure the audit event as appropriate.

Audit records resulting from this audit event contains the following detail:

- time of occurrence;
- identity of requester (IP address);
- facility source (domain name, if available);
- severity code;
- event identifier.

References

"Information Assurance Advisory No. IAA-003-1999," subject: "Information Assurance (IA) – More Than Evaluated Products," dated 3 November 1999, and signed by Michael J. Jacobs, Deputy Director for Information System Security

"Information Assurance Technical Framework," Release 2.0.1, September 1999, Issued by the National Security Agency, Solution Development and Deployment, Technical Directors

"X.509 Certificate Policy for the United States Department of Defense", dated 13 Dec 1999

"Department of Defense Chief Information Officer Guidance and Policy Memorandum No. 6-8510 Department of Defense Global Information Grid Information Assurance", dated 16 Jun 2000

Common Criteria Implementation Board, "Common Criteria for Information Technology Security Evaluation, CCIB-98-026", Version 2.0, May 1998

Skyline Systems, "Secure Remote Access System, Skyline Community Manager User Guide, Appendix E" – Cryptoserver Event Messages

Centrac Corporation, "Windows NT 4.0 Security Event Logging Assessment, Recommendation Report, DRAFT"